IDENTITY MANAGEMENT POLICY AND UNLINKABILITY: A COMPARATIVE CASE STUDY OF THE US AND GERMANY

GILAD L. ROSNER

Thesis submitted to the University of Nottingham for the degree of Doctor of Philosophy

July 2014

ABSTRACT

This study compares the privacy policies of Germany and the US in the field of identity management. It analyses the emergence of unlinkability within the countries' electronic citizen identity initiatives. The study used qualitative research methods, including semi-structured interview and document analysis, to analyse the policy-making processes surrounding the issue of unlinkability. The study found that unlinkability is emerging in different ways in each country. Germany's data protection and privacy regimes are more coherent than the US, and unlinkability was an incremental policy change. US unlinkability policies are a more significant departure from its data protection and policy regimes. New institutionalism is used to help explain the similarities and differences between the two countries' policies. Scholars have long been calling for the use of privacy-enhancing technologies (PETs) in policy-making, and unlinkability falls into this category. By employing PETs in this way, German and US identity management policies are in the vanguard of their respective privacy regimes. Through these policies, the US comes closer to German and European data protection policies, doing so non-legislatively. The digital citizen identities appearing in both countries must be construed as commercial products inasmuch as official identities. Lack of attendance to the commercial properties of these identities frustrates policy goals. As national governments embark on further identity management initiatives, commercial and design imperatives, such as value to the citizen and usability, must be considered for policy to be successful.

ACKNOWLEDGEMENTS

I could not have accomplished this thesis without the help of many wonderful people. First and foremost I wish to thank my supervisors, Prof. Stephen Cope and Dr. Andrew Greenman, who guided me through the academic fog with patience and firmness. Next, I would like to thank Prof. Sarah Sharples, Prof. Steve Benford and Prof. Derek McAuley who supported me generously throughout my research. I am also grateful to Nick Mothershaw and Jim Purves of Experian, whose ideas greatly influenced my research in its earliest stages. I am indebted to David and Anne Bergman who let me move back in with them one last time to undertake my US field research. I also wish to thank my mentor and friend, Prof. Martin Elton.

My return to academic life and the production of this research was bound up in my departure from the United States to live abroad for the first time. The transition was challenging, and would have been harder but for the excellent new friends I made upon moving to England. I am ever grateful for the support and friendship of Nik and Finbarre Snarey, Jo and David Breeze, and Aaron Collins. The US was never far from my mind, and I was supported in my endeavours at a distance by Ashton Applewhite, Joshua Rubin, Gilad Gabbay, Cheryl Hurst and Kia Meaux. I am particularly grateful for the encouragement and support of Elizabeth Varley.

I was extremely fortunate to be in the company of the inaugural cohort of the Horizon Doctoral Training Centre. I am very thankful for the warm friendship and thoughtful advice of Ewa Luger and Michael Golembewski.

Finally, I wish to thank my parents, Debbie and Efraim, whose love and unswerving support has followed me all of my days.

LIST OF CONTENTS

Abstract **2**

Acknowledgments **3**

List of Contents **4**

List of Figures and Tables **8**

Chapter 1: Introduction **10**

Research Aims and Questions *15*

Theoretical Framework *17*

Significance of Study *19*

Thesis Structure *24*

Chapter 2: Theoretical Perspectives: Information Policy and New Institutionalism **25**

Information Policy: Definitional Problems *26*

Disciplinary Ghettos *30*

The Purpose of Information Policy *31*

Theoretical Weaknesses of Information Policy *33*

Information Policy Sub-topics *36*

Theoretical Approach *37*

The 'Old Institutionalism' *42*

The New Institutionalism *43*

The Variants *45*

A Holistic Approach to Institutional Analysis *48*

The Core Propositions of Institutionalism *49*

Various Definitions of Institutions *50*

Synthesis of Institutionalisms *52*

Data Protection as an Institution *58*

Institutional Change *61*

Application of New Institutionalism to Empirical Data *63*

Chapter 3: Methodology **66**

Overview *66*

Research Aims *66*

Research Methods *68*

Data Collection *75*

Analysis *79*
Ethics *82*
Summary *82*
Chapter 4: Key Terms and Concepts **85**
Introduction *85*
Unlinkability *87*
What is digital identity? 87
What is identity management? 92
What is federated identity? 98
The ID spectrum 102
What is unlinkability? 107
Citizen Credentialing *112*
Conclusion *117*
Chapter 5: Unlinkability in US Information Policy **121**
Introduction *121*
Overview *123*
Early Government Identity Federation *124*
E-Government Priorities *125*
Exposure to British Policy Models *126*
Acceptance of External Credentials *127*
Public-Private Authentication Initiatives *130*
Establishment of FICAM *131*
Creation of Trust Frameworks *132*
Identity Scheme Adoption *134*
Pseudonymous Identifiers *135*
Privacy Criteria *136*
FIPPs in FICAM *138*
Cybersecurity Policy Review *140*
OpenID and the Open Identity Exchange *141*
National Strategy for Trusted Identities in Cyberspace *143*
Federal Cloud Credential Exchange *149*
Policy summary *152*
Themes *153*
National ID *154*
Relationship to minimisation *155*

Spectrum of enforcement *156*
Relationship to Activity Tracking *157*
Translating the physical world to the electronic *158*
Commercial influences *159*
Need for personal data to conduct business 160
Need for business cases in citizen identity management 161
Multiple Markets 164
Variation: Higher Education 165
When Linkability is Good 167
Technical vs. social methods of privacy enforcement *168*
Privacy at the protocol level *171*
The challenge is not technical *172*
Comparability vs. compliance *172*
Actors *174*
Usability *175*
Conclusion *179*

Chapter 6: Unlinkability in German Information Policy 182
Introduction *182*
Overview *184*
E-government Initiatives *185*
Introduction of the e-ID: Policy history, rationale and intentions *187*
Features 191
User interaction 192
Data protection model 193
Pseudonymity function 196
Policy Summary *198*
Themes *200*
Informational self-determination *201*
Privacy mindset *209*
Stronger protections for validated data *211*
Relationship to e-passport *213*
Commercial influences *214*
Technical vs. social methods of privacy enforcement *217*
Marketing *219*
Policy actors *221*

Usability *225*
Conclusion *227*

Chapter 7: Comparison of German and US policies **230**
Introduction *230*
Policy requirements *234*
Technical implementation *240*
Pre-FCCX 242
Post-FCCX 244
Data protection models *246*
Actors *249*
Commercial influences *254*
Implementation Challenges *257*
Defining Identity Management Policy *260*
Conclusion *263*

Chapter 8: Applying New Institutionalism to Unlinkability **267**
The choice to include unlinkability in citizen credentialing is influenced by formal and informal mechanisms. *272*
There is a taken-for-granted quality to the policy of unlinkability. *278*
There is an isomorphic dimension to the choice to require unlinkability. *281*
Prior policy choices constrained and affected the choice to require unlinkability. *286*
Networks of social actors influenced the policy of unlinkability. *292*
Material artefacts further institutionalise data protection. *297*
Institutional Change *304*
Conclusion *307*

Chapter 9: Conclusion **311**

Appendix A: List of Interview Subjects **329**
US Case Interview Subjects *329*
German Case Interview Subjects *330*

Appendix B: Topic Guide **331**
Regulation *331*
Technical *332*

Bibliography **334**

LIST OF FIGURES AND TABLES

Figure 2.1 Three pillars of institutions 52
Figure 2.2 Institutional pillars and carriers 55
Figure 2.3 Map of institutional change explanations 63
Figure 3.1 Spectrum of credential issuance sources 72
Table 3.1 Frequency of respondent references 80
Figure 4.1 Nested topics to understand unlinkability 86
Figure 4.2 The identity management lifecycle 94
Figure 4.3 Individual authentication versus identity authentication 95
Figure 4.4 Two-factor authentication 97
Figure 4.5 Federated identity 100
Figure 4.6 Federated identity: university and publisher relationship 100
Figure 4.7 Authoritative versus non-authoritative identity relationships 102
Figure 4.8 The ID spectrum 103
Figure 4.9 Unidirectional versus omnidirectional pseudonyms 106
Figure 4.10 Pairwise persistent pseudonyms 108
Figure 4.11 Federated identity with a proxy: the US Federal Cloud Credential Exchange 110
Figure 4.12 Matrix of credential type and issuance 115
Figure. 5.1 Impact category/Level of Assurance matrix. 128
Figure 5.2 A Trust Framework 133
Figure 5.3 Proposed Federal Cloud Credential Exchange 150
Figure 5.4 Reed's spectrum of unlinkability 156
Figure 5.5 US IDM privacy efforts in relation to Reed's spectrum 169
Figure 6.1 The original paper laminated national ID card 187
Figure 6.2 The new e-ID card 188
Figure 6.3 AusweisApp screenshot: requesting service provider information 192
Figure 6.4 AusweisApp screenshot: requested personal data 193
Figure 6.5 The e-ID pseudonym generation process 196
Figure 6.6 The e-ID logo 221
Figure 7.1 Pairwise pseudonyms 236
Figure 7.2 The e-ID pseudonym generation process 240

Figure 7.3 The redirect method: User begins at service provider 243
Figure 7.4 Proposed Federal Cloud Credential Exchange 245
Figure 7.5 Reed's Spectrum: US and German policy instruments and influences 248
Figure 8.1 Location of Germany and US on map of institutional change explanations.....306

CHAPTER 1: INTRODUCTION

This first chapter introduces the core subject matter, problem space, research aims, and research questions of this thesis. It then briefly introduces the theoretical approach, which is explained in detail in Chapter 2. The final section details the overall structure of the thesis.

The internet was born without an identity layer. The capacity to identify people was not built into the core protocols of the internet. Successful sending and receiving of messages was the critical consideration. Identification was a local phenomenon, specific to each organisation's needs and practices. People were given usernames and passwords, one for each resource or organisation. These were the earliest digital identities (Organization of Economic Cooperation and Development [OECD], 2007, pp. 41-42).

As the internet became commercial, identification was a matter of personalisation. It was helpful to website owners to know who was returning to make her or his online experience richer. As the web proliferated, so did the number of usernames and passwords. 'The password problem' was recognised – people have too many, and they manage them insecurely (Small, 2004). The next evolution in digital identity was the use of the same username and password for multiple resources. The username and password became a *single sign-on* – login once, use for many applications. Soon after, logins could be used for disparate resources external to the host organisation. This is known as *federated identity*. The originating source of a digital identity was called the *identity provider*; those who relied on their *identity assertions* were called *relying parties.* This addressed the password problem because it allowed fewer logins to be used for many activities.

Alongside these innovations in digital identity, governments were putting more resources and information online. Meaningful e-government – such as exchanges of tax data, health data, court information, benefits information – usually requires an exchange of personal information. North American and

European governments mandate privacy and protection for personal data in many contexts, especially in citizen-government relations. To conduct business online, government needed to know who was at the other end of the screen; they needed to *authenticate* citizens. The absence of an identity layer in the internet posed challenges to this need. The appearance of federated identity was a potential solution.

Federated identity has inherent privacy challenges (Landau, Le Van Gong and Wilton, 2009). When one entity, the identity provider, vouches for the identity of a person at multiple websites, the identity provider knows where the person went online. The promise of simplified logins is counterbalanced by the profiling of users' activities. When you use an identity provider, 'someone is always looking over your shoulder' (N005, Interview). This is true in both commercial and government contexts. Governments could not address their identity problems without considering these challenges. More broadly, as identity transactions on the internet increased and sources of identity became more concentrated, people's online activities became more linked, and profiling became easier.

Given the broad duty to protect the privacy of their citizens, governments are adapting to the growth of an identity layer and its inherent challenges. They have greater sway within their own dominion of e-government than in the commercial domain, but national policies have begun to reflect concern over the profiling that is possible as the internet becomes a more identifiable place. Law and policy are notoriously out of step with technological change – "today's regulations may easily pertain to yesterday's technologies" (Reidenberg, 1997, p. 586). Identity technologies are complex and obscure, propelled forth by commercial interests and the work of standards bodies. The impulses that underpin data protection regimes are being re-applied and innovated to meet the privacy challenges new identity technologies pose.

The question remains, though, how much can regulation and policy affect the privacy landscape? A deterministic reading of internet technology would seem

to support Scott McNealy, former Chief Executive Officer of Sun Microsystems, who in 1999 infamously said,

> "You have zero privacy anyway. Get over it." (Sprenger, 1999).

The great computer trends of recent years are predicated on networking, sharing, storing and mining data. Information processing also yields a tremendous amount of logging to ensure that systems perform correctly. The widespread intentional sharing of data and the porousness of boundaries between organisations, systems and contexts challenge those who seek to strengthen privacy regimes. The centralisation of identity transactions amplifies the problem by making people more identifiable, potentially clashing with the internet's historically pseudonymous character.

Much research and standards development in the field of identity management (IDM) occurred through the early and mid-2000s, often with a focus on privacy. In 2004, the Privacy and Identity Management for Europe (PRIME) project was launched with an explicit goal "to develop a working prototype of a privacy-enhancing Identity Management System" (PRIME, 2008). In 2005, Microsoft identity architect Kim Cameron published his "Laws of Identity" as part of his work on an 'identity metasystem' that would give users greater control over their digital identities. Microsoft created CardSpace, an implementation of Information Cards, a user-centric identity management model (Chappell, 2006). PRIME was succeeded by PrimeLife, with a specific goal to help "maintain life-long privacy" (PrimeLife, n.d.). Standards such as OpenID (OpenID Foundation, n.d.) and SAML (OASIS, 2013) appeared and evolved, both ultimately containing privacy-enhancing features. The work of Ann Cavoukian, Information and Privacy Commissioner of Ontario, and others on 'privacy by design' was incorporated into identity management literature (Cavoukian, 2006). The Future of Identity in the Information Society (FIDIS) project launched to help "Europe … develop a deeper understanding of how appropriate identities and identity management can progress the way to a fair(er) European information society" (FIDIS, n.d.).

All of the above research and standards addressed privacy concerns. In particular, this body of work and related scholarship recognised the criticality of pseudonymity. Privacy goals of data minimisation, the separation of different social contexts, and the frustration of illegitimate profiling are assisted by pseudonyms (Independent Centre for Privacy Protection and Studio Notarile Genghini [ICPP and SNG], 2003). When an identity management system uses different pseudonyms to represent a user in separate contexts, the term '*unlinkability'* is used, referring to the breaking of 'links' that connect a user's online activity to her or him. Ideal types of identity management systems made frequent reference to unlinkability and pseudonymity (Camenisch, et al., 2005; Storf, Hansen and Raguse, 2009), and IDM standards like OpenID and SAML included the capability to create unlinkable credentials. Advanced cryptographic systems such as Microsoft's U-Prove and IBM's idemix had privacy principles built into their core architectures, including unlinkability and selective disclosure of attributes (Paquin, 2013; Camenisch and Van Herreweghen, 2002). Unlinkability is part of the family known as 'privacy-enhancing technologies' (PETs), and calls for such technologies to be included in policy and commercial products have appeared in academic literature (Clauß, Kesdogan and Kölsch, 2005; Clauß and Köntopp, 2001; Koops and Leenes, 2005; PrimeLife, 2009; Reidenberg, 1997).

This thesis is about the translation of the values, research and technology of PETs into public policy. It explains how unlinkability has emerged in Germany and the United States. Calls for unlinkability by researchers, technologists and data protection practitioners have been echoed in agency position documents, national strategies, international research and supranational regulations. The US Federal Trade Commission discussed the privacy challenges of linkability in its 2012 report, *Protecting Consumer Privacy in an Era of Rapid Change*. The White House (2012) championed a Consumer Privacy Bill of Rights which contained data minimisation principles that could be aided by unlinkability. The US National Strategy for Trusted Identities in Cyberspace took a clear position on such issues:

> "The Identity Ecosystem will use privacy-enhancing technology and policies to inhibit the ability of service providers to link an individual's transactions, thus ensuring that no one service provider can gain a complete picture of an individual's life in cyberspace." (White House, 2011, p. 2).

The Organisation for Economic Coordination and Development (OECD), whose 1980 data protection guidelines are a foundation for much modern data protection policy (Gellman, 2012), published a primer for policy-makers on identity management, stating:

> "Identity systems that facilitate anonymity and pseudonymity may offer promise. Their deployment would raise issues regarding who has the right to decide which data should be veiled and the circumstances under which it might be unveiled. This is of particular importance to the exercise of free expression, free association, and the security of the person." (OECD, 2009, p. 14)

German internet law requires the option for pseudonymous use of internet services (Telemedia Act, 2007, Sec. 13(6)). It is aligned with German data protection law's pseudonymity requirements (Federal Data Protection Act, 2003, Sec. 3a); this is covered in depth in Chapter 6. The 2012 draft regulation intended to update the 1995 EU Data Protection Directive promotes the use of pseudonyms (Albrecht, 2013). In a 2013 speech, Viviane Reding, Vice-President of the European Commission, stated:

> "We should encourage companies to use pseudonyms rather than the actual names of persons. This makes sense. It is in the interest of citizens." (Reding, 2013)

Statements such as this and government encouragement of PETs appear at a time when citizen concern over losses of privacy is increasing (Eurobarometer, 2011). The breadth of national surveillance activities has been thrust into the spotlight after the high profile leaks of classified documents by Edward Snowden, a former contractor to the US National Security Agency (Greenwald and MacAskill, 2013). This follows more than a decade of increased cybersecurity initiatives accompanied by weakened privacy protections in the wake of the terrorist attacks of September 11th, 2001 (Lyon and Haggerty, 2012). Identity management policies and the evolution of privacy-enhancing technologies are counter-currents to these trends. They are a competing

narrative and set of priorities within government. The prerogative of law enforcement and the encouragement of PETs represent tension between the state's desire to know and to *not* know about its citizens; a tension between legitimate and illegitimate informational intrusion. The transformation of IDM privacy policy goals into implementable solutions and the challenges therein, and the institutional forces influencing those goals, are the subject of this thesis.

Research Aims and Questions

The research aims are two-fold:

- Examine how governments are addressing the privacy challenges inherent in the use of new identity technologies through the strategy of unlinkability

- Examine the interplay of government, market and technological imperatives within national identity management initiatives

The first aim of this study is to examine the policy mechanisms that governments are employing to address the privacy challenges inherent in the use of new online identity technologies. The goal is to understand how privacy interests are emerging as public policy in relation to evolving identity technologies. Data protection is accomplished through a variety of policy instruments, and this study examines two countries' initiatives to apply those instruments to the new field of identity management. This field is subject to multi-stakeholder governance, lying at the intersection of public policy, business and technical standards, so policy-making must encompass a wide variety of interests and influences. The study traces the policy development of a modern privacy interest – unlinkability. It is a specific strategy to effect the data protection goals of proportionality and minimisation, increase user control over personal information, separate informational contexts, and frustrate illegitimate profiling. This study will examine the question of how unlinkability is emerging as public policy in Germany and the US.

The second purpose of the study is to examine the interplay of government, market and technological imperatives within national identity management

initiatives. To accomplish this, the study analyses large-scale efforts to supply citizens with digital credentials to use on e-government and commercial websites. This analysis aligns with the first research aim above as unlinkability is a strategy and technical architecture that occurs within IDM systems.

This thesis adds to the limited body of empirical research on policy-making processes related to identity management and PETs. Regarding identity management research generally, Halperin and Backhouse (2008, p. 12) note:

> "Empirical studies are emerging but so far are the minority, as perhaps might be expected, but the focus, by turns, is shifting from the technological artifact *per se* to the social, legal and cultural hinterland in which the technology thrives…."

Further, the strategy of unlinkability in national information policy is an under-researched area (Aichholzer and Strauβ, 2010; Noack and Kubicek, 2010). In part, this is a reflection of the dearth of PETs being used as policy instruments. Koops and Leenes (2005, p. 187) observe:

> "… PETs by and large seem a pet of data protection commissioners and privacy lobbyists, but so far they do not seem to get through to others. They remain a mainly theoretical solution that has yet to prove its effect in practice."

This thesis yields new knowledge by exploring in depth the rare appearance of PETs in national information policy. The study ties historical data protection principles to current identity management policy problems, and analyses the institutional effects that influenced such policy-making. Moreover, there is no academic literature on US credentialing initiatives for citizen access to e-government. This thesis yields new knowledge by analysing these initiatives, and then comparing them to those of Germany.

German and US identity management policy did not formally influence one another. Despite this, both countries have developed policies of unlinkability in their citizen credentialing initiatives in similar timeframes. Given the lack of formal policy influence on one another, an explanation of the similar appearance impels an examination of informal influences such as relationships among actors, norms, lexicons, international standards, and cultural factors.

Further, information policy scholarship decries a lack of theoretical approaches within such research, and calls for attendance to norms, values and the institutional dimensions of policy-making (Browne, 1997a; Rowlands, 1996; Trauth, 1986). The theoretical approach of *new institutionalism* analyses informal influences and values, as well as the formal influences of laws, rules and court decisions. The Theoretical Framework section below expands on the utility of new institutionalism.

To address the research aims, the following questions are posed:

- How is unlinkability emerging as public policy in Germany and the US?
- What is the relationship between unlinkability and historical privacy and data protection regulations?
- What are the similarities and differences between US and German unlinkability policies?
- To what extent can new institutionalism explain the emergence of unlinkability?

These questions mandate examining policy requirements for unlinkability in credential architectures for citizen digital identities. The research will explore the formal policy instruments, their genesis, history and influences, relationship to prior policy instruments, and technical implementations. It will examine the informal influences of values, relationships, common lexicons, and cultural phenomena. Unlinkability is a characteristic of a technical system, so the research necessarily explores the context in which it appears: citizen credentialing. As such, this thesis is also a detailed examination of German and US initiatives to provide their citizens and residents with online credentials for use with e-government and commercial websites. In doing so, it examines the institutional role of the material technologies of credentialing systems.

Theoretical Framework

While a comparison of the formal policy instruments and their implementation is a fruitful endeavour, a full accounting of the emergence of unlinkability

benefits from an analysis of the informal influences on policy development. Information policy literature decries the theoretical poverty of the field, and instead calls for attendance to institutional factors of policy-making, and examination of the values and norms influencing policy (Browne, 1997a; Rowlands, 1996; Trauth, 1986). Also present in this literature is the view that information policy scholarship is fragmented and discipline-bounded (Browne, 1997a; Rowlands, 1996; Trauth, 1986). Halperin and Backhouse (2008) find the same to be true for the broader emerging field of digital identity research. They observe:

> "… interdisciplinary research seems desirable, indeed necessary, for achieving a multifaceted and rounded understanding of the identity domain. However this is not the prevailing trend. Research in identity is currently fragmented along disciplinary lines." (Halperin and Backhouse, 2008, p. 13)

To answer these calls for greater use of theory, attendance to norms, values and institutional factors, and discipline-spanning research, an institutionalist theoretical approach is applied to the case data. The broad church of new institutionalism is used to analyse the institutional influences underpinning the privacy regimes of German and US citizen credentialing efforts, and examine the role of norms and values in IDM policy-making. This analysis includes the formal instruments of policy, such as laws and government technical specifications, and the informal influences, such as culture, lexicons, common mindsets, and relational networks. The analysis conceptualises data protection as an institution, and thereby able to be examined as a process that is influenced by a plurality of formal and informal forces. Human actors and material technologies enact this institution, and it exerts an influence on identity management policy while also being affected by it; this dual role is characteristic of institutions (Katzenbach, 2012). Credentials – both 'soft' ones and those based on cards – further institutionalise data protection among the German and American polities by concretising data protection principles within their technical architectures.

Institutionalist analysis helps to explain the past, present and future of unlinkability. It does so by incorporating cultural influences and material

artefacts into an explanation of the emergence of unlinkability as public policy. The empirical material provides insight into policy development processes and the theory helps to develop an explanation of the institutionalisation of data protection for IDM and the use of PETs. New institutionalism draws upon economics, sociology, organisational theory and political science. This interdisciplinary character comports well with calls in information policy and identity management scholarship for integrative approaches to research. This thesis contributes to information policy by applying an institutionalist approach to introduce further social theory into the field, as well as examine institutionalism's suitability as an explanatory framework. It contributes to institutionalist scholarship by applying it in a novel empirical domain – identity management. New institutionalism and the rationale for applying it are the subject of Chapter 2.

Significance of Study

This thesis explores the reapplication of core data protection and privacy principles in the field of identity management. Concern over privacy in the online world is on the rise (Eurobarometer, 2011). The internet is no longer an experiment – it is a social space in which an estimated one third of the world's populace interacts (Internet World Stats, 2013). A key characteristic of the internet is its ability to link data, resources and people together; this can be both valuable and harmful. Privacy researchers have long spoken of technology's 'panoptic gaze' into the lives of all whom it touches (Gandy, 1993; Reiman, 1995). As more people use the internet and as identity technologies evolve, the breadth and depth of profiling increases, as does the potential for people to lose control over their digital identities.

Another key characteristic of the internet is that its inner workings are invisible. This invisibility combined with linkability and logging, a by-product of information systems, lays bare the online activities of millions of users, most of whom are unaware of the breadth of data collected about them. Commercial companies' appetite for consumer data adds an urgent pressure to this collection. At the root of concern is identifiability, as that ties profile data to

individual people. The field of identity management lies at the intersection of concerns over profiling, identifiability, privacy and user control. Born of the need to correctly match user accounts with their owners, identity management has become an important component of the increasingly electronic character of human interrelations and political phenomena.

This study examines how regulative instruments can be brought to bear in this more identifiable internet; how historic impulses to protect privacy are being reinterpreted and reapplied. It examines a particular application of privacy-enhancing technologies – long touted as critical tools – as a deliberate policy initiative. Identity management and its privacy challenges are the subject of a great deal of research, and much of it calls for privacy to be designed into systems at a fundamental level (Cavoukian, 2006; Hansen, 2008a, 2012; Leenes, 2008). This study examines government attempts to do that in the realm of citizen credentials. It tests normative arguments for privacy against the empirical complexities of policy-making and the constraints of competing government, technological and commercial imperatives. By approaching the data through the theoretical lens of neo-institutionalism, unlinkability can be seen to emerge through formal instruments, technical artefacts and informal modes of policy-making.

A small amount of literature exists on the policy-making process of the German e-ID and its online authentication features (Hornung and Roßnagel, 2010; Noack and Kubicek, 2010). This scholarship touches upon its unlinkability features, but only superficially; its main concerns are the technical and political aspects of the e-ID's ability to authenticate its bearer online. The present research explores unlinkability's nature and genesis with more rigour by placing it in historical context within the institution of data protection, and by examining the norms and values that helped to shape the policies. A comparative policy study is used, drawing upon institutionalist theory to examine the processes through which unlinkability is emerging. This research also subjects the German process of certifying access to personal data

stored on the e-ID to the same degree of contextual, value-critical and comparative study.

As to the US case, there is very little academic literature on American citizen credentialing efforts, and all of it is focused on credentials for non-governmental access (Adjei, 2013; Grant, 2011; Katzan, 2011a, 2011b; Schwartz, 2011). The empirical data and subsequent analysis of US initiatives adds to the mainly European body of scholarship on national identity management. Political, technical and institutional analyses of US IDM efforts contribute much needed research to this new sub-field of information policy. With regard to privacy research, much normative literature exists on pseudonymity and unlinkability, but there is limited empirical data on government efforts to enact specific policies (Aichholzer and Strauβ, 2010; Mariën and Van Audenhove, 2010; Noack and Kubicek, 2010; van der Hof, Leenes and Fennell, 2009). Research on public policy development and implementation of these privacy goals is critical for holistic scholarship in identity management. In conducting such research, the thesis broadens knowledge about the journey of privacy values to their codification in social policies. This research is also significant for its synthesis of US and European IDM lexicons and concepts into forms and examples suitable for analysis by non-technical information policy scholars.

Identity management research has been approached from legal, technical and sociological viewpoints (ICPP and SNG, 2003; Storf, Hansen and Raguse, 2009). Political science approaches, however, are under-researched (Kubicek, 2010). This thesis addresses this gap. Further, much academic literature is published in the form of journal articles, reports and edited book chapters. Empirical data is often submerged, and instead scholars offer syntheses of the data. The length of PhD theses allow for much more empirical data to be exposed to readers, providing a richer experience and a greater opportunity to assess validity of the work.

The core contribution of this thesis is an analysis of the process through which unlinkability – and thereby, PETs – are appearing in the information policy of Germany and the United States. Actors in both countries set out to provide online citizen credentials with high degrees of confidence in their authenticity. This is part of each country's identity management policy, a sub-field of information policy concerned with the creation, use and privacy of citizen credentials. Specific policy choices by administrators led to the inclusion of unlinkability among the privacy features of national credentialing systems. These choices are among the most forward-looking national privacy policies in both countries.

Prior academic literature does not synthetically define national identity management policy-making. A key contribution of the thesis is this definition: *Identity management policy is the set of laws and policies enacted by governments and supranational bodies concerning the facilitation, procurement, use, liability, legal nature, interoperability, technologies, risk methodologies, lifecycle and privacy of digital identities for its citizens and employees. This includes physical and logical authentication, e-signature, and electronic identification technologies for access to physical and electronic resources.* The definition is explicated in Chapter 7.

This thesis argues that data protection is an institution – a repeating pattern of social action that does not need extraordinary effort to maintain it. The research examines how the institution of data protection is exerting a strong influence on the development of identity management policy in Germany and the US, contributing to the emergence of unlinkability. Identity management policy-making is inherently technocratic due to its reliance on complicated technologies and concepts. Privacy concerns relating to digital identities did not rise to the level of legislatures in the two countries, leaving such policy to administrative and bureaucratic levels. This, plus the inclusion of data protection practitioners, technologists, standards developers and consultants allowed a set of privacy-conscious values to guide policy-making and become embedded in technical systems. Investigating unlinkability leads to an

examination of policy processes that are not often visible in the final outputs of legislatures. This study thereby contributes to information policy research by broadening the empirical base from which to analyse how national privacy regimes develop.

Digital identities, from either state or private sources, differ from classic official identities such as national ID cards. Digital identities are products, and therefore subject to market influence. In the US case, where policy-makers hope that private organisations will supply credentials to the citizenry, this product nature is paramount. In Germany, where credentials are non-mandatory and built upon a national e-ID, the need for product marketing is evident in the slow take-up of the credentials. The two case studies illustrate how inattention to market considerations can harm policy goals. Overall, by tying its policy implementation to private actors, the US is more susceptible to a conflict of market and government rationales than Germany.

Digital identity is also tied to risk management. The risk to be managed is the certainty that the correct person is using an identity credential. The US case fully illustrates this risk perspective through its policy reliance on credentials that are produced and managed by private actors. To harmonise government agencies' ability to judge a credential's authenticity, a risk management methodology called the 'Levels of Assurance' was built. In the German case, a similar methodology is in formative stages to enable German digital identities to be used in other European countries. The risk-bound nature of digital identity highlights that identities are 'local' – organisationally-derived – and the crossing of organisational boundaries requires a framework in order to trust the credential. These risk management characteristics of digital identity are under-researched in identity management scholarship. This thesis adds to new knowledge by exploring the relationship between identity credentials and risk management strategies in Germany and the US.

Thesis Structure

The thesis is structured into nine chapters plus bibliography and appendices. The first chapter is this introduction. The second chapter sites the research in the multidisciplinary field of information policy. This chapter also explains and justifies the use of the new institutionalist theoretical approach. The third chapter explains the methodology of the research. The fourth chapter supplies the reader with the key terms and technical concepts needed for an exploration of unlinkability. The fifth chapter is the empirical data for the US case. It is broken into Policy and Themes sections. The sixth chapter is the empirical data for Germany, structured identically to the US chapter. The seventh chapter is a comparison of the policies and implementations of the two countries. The eighth chapter is the application of new institutionalism to further explain the emergence of unlinkability. The final chapter contains overall conclusions of the research and suggestions for future research into identity management policy.

CHAPTER 2: THEORETICAL PERSPECTIVES: INFORMATION POLICY AND NEW INSTITUTIONALISM

This chapter will expand on how unlinkability can be examined as an example of the developing identity management policy of Germany and the US. This thesis is rooted within the field of information policy as the research aims and questions focus on topics typically examined within information policy research. These include data protection, privacy, identity management and e-government practices. The empirical research investigates how the US and German governments are building identity management systems for citizens, their privacy architectures, and the values, norms and goals embedded within them. Specifically, the strategy and architecture of unlinkability is examined. The formal policies behind these IDM systems consist of laws, regulations, court decisions, administrative and bureaucratic choices, protocols and standards, and technical choices. The informal influences include values, norms, relationships, narratives and cultural phenomena. All these policy elements are embedded within and affected by institutions such as data protection, the market, and the state. The institution of data protection influenced US and German choices to require unlinkability within their citizen credentialing systems. This chapter will explain the theoretical basis from which these influences will be analysed in the empirical material.

The chapter begins with a review of the domain of information policy, highlighting its definitional and disciplinary challenges. It goes on to examine its under-theorised state and related calls for taking account of the institutional dimension of policy-making. Information policy embraces formal and informal rules, expectations and norms. These qualities suggest that the 'new institutionalism' theory is well-suited for information policy research as it emphasises analysis of the informal versus the formal, norms, narratives, and values. The chapter explicates this theory, and illustrates how it is applied to the empirical material. The chapter concludes by conceptualising data protection as an institution, and arguing that the choice to include unlinkability in citizen identity management systems can be fruitfully explained by an

application of institutionalist thought. A synthesis of the various branches of new institutionalism based on the work of Scott (1995, 2003, 2008, 2010) and Lowndes (1996, 2010; also Lowndes and Roberts, 2013) is used. To facilitate analysis, this work is distilled and applied to the empirical research in the form of seven institutionalist propositions. These are used to explain the process through which unlinkability emerges and forms part of German and US identity management policy.

This chapter also surveys the use of institutionalism in information policy generally. There is little academic literature on the institution of data protection, and less on how material technologies reify the norms and values of it. There is a small amount institutional analysis of identity management (Aichholzer and Strauβ, 2010; Kubicek, 2010; Noack and Kubicek, 2010). This research addresses these gaps using new institutionalism to provide a more theoretically-informed analysis of the emerging sub-field of identity management policy research. Doing so contributes to a holistic explanation of the emergence of unlinkability in Germany and the US, and illustrates the intersection of government, market, standards and technology in the policy-making process. This further contributes to information policy scholarship's theoretical development, and the development of new institutionalism by testing it against novel empirical data.

Information Policy: Definitional Problems

Information policy is a heterogeneous field. A consistent theme in information policy literature is the difficulty of defining it. Information policy is "contested ground … a moving target" (Doty, 1998, p. 59), a "fuzzy set" (Overman and Cahill, 1990, p. 803; Rowlands, 1996, p. 14); it has "porous boundaries" (Browne, 1997a, p. 270), and is "fragmentary, overlapping and contradictory" (Rowlands, 1996, p. 14, quoting Hernon and Relyea). Several attempts have been made at defining information policy. Weingarten (1989, p. 79) described it as "the set of all public laws, regulations, and policies that encourage, discourage, or regulate the creation, use, storage, and communication of information." In later work, he specifically included informal policies, such as

organizational rules, standards and guidelines, mores and norms, as well as formal policies such as constitutions, laws and regulations (Weingarten, 1996, p. 45). Burger (1993, p. 6) defined information policy as "societal mechanisms used to control information, and the societal effects of applying those mechanisms." Trauth (1986, p. 41) called it

> "… the set of activities currently in existence which aim to achieve certain goals in the realm of information processing and communication. The goals may either be implicit or explicit."

Doty (1998, p. 60) calls information policy "the collection of laws and policies dealing with information from its creation, through its collection, organization, dissemination, and repackaging, to its destruction." Braman states that the information policy field includes "government … governance … and governmentality," (2009, p. 3) and that it appears "at the intersection of informational, technological, and social structures" (2009, p. 6). Given these definitional challenges, Duff (2004, p. 70) observed that "information policy suffers from disciplinary territorialism, conceptual underdevelopment, and … the absence of a widely accepted definition."

The survey of definitions above yields a number of common themes. There is widespread agreement that a foundational element of information policies is the set of formal laws, policies or regulations within a given policy context; that information policy, near its heart, is (at least partly) concerned with constitutions, the products of legislatures, court decisions, regulations and the formal rules of state-based agencies. The more inclusive definitions above cite 'norms' or 'societal mechanisms' – these can arguably be contrasted with Trauth's assertion that information policies "aim to achieve certain goals" (1986, p. 41). As will be further discussed below, policies that derive from norms may not be goal-oriented. The inclusion of norms and mores in a definition of information policy is critical; according to Braman (2009, p. 5):

> "It is a classic analytical error … to believe that it is possible to understand what is happening to society via the use of information policy to exercise power by looking at only laws and regulations."

Yusof, Basri and Zin (2010) take a classification approach to describing the boundaries of information policy. Based on a literature review, they identify 91 issues underlying information policy and classify them into 6 groups: technical and scientific information, library, information and communication technology, social issues, government information, and economy (Yusof et al., 2010, p. 207). They argue that this classification of issues has not changed since the "earliest research" (2010, p. 205), only the variety of issues within those groups. They conclude that information policy is "a multidiscipline of its own" (2010, p. 210), echoing earlier work by Duff (2004). They cite the fluidity with which researchers of various disciplines rely on scholarship from outside their own fields: "Differences in background did not limit debates and acceptance of issues presented by researchers in different disciplines" (2010, p. 210). However, Rowlands (1996, pp. 19-20) argued that while classification-based approaches to information policy research are useful given its very broad scope, he decries them for their theoretical poverty:

> "While there may be some practical benefits in a classification-based approach to information policy, there is little to recommend this approach from a theoretical standpoint: classification can only deal with policy in a very superficial way, obscuring the political, social, and institutional contexts within which policy is shaped and implemented. A more fundamental objection is, that by classifying policies into mutually exclusive categories, we risk losing a sense of the interrelationships between groups of issues."

Rowlands' points can be illustrated with an example from US law. The USA PATRIOT Act was enacted soon after the terrorist attacks of September 11, 2001. Section 215 of the Act amends the Foreign Intelligence Surveillance Act (FISA) to allow FISA court orders to apply to a wider array of businesses and organisations – interpreted to include libraries. These orders can compel organisations to grant access to "*any tangible item no matter who holds it*, including by implication library loan records and the records of library computer use" (Doyle, 2003, p. 1). This provision has been criticised by parts of the US library community as an infringement on constitutional rights and privacy (ALA, n.d.). In Yusof, Basri and Zin's classification above, research on this topic would minimally fall into both the library and social issues categories. Rowlands' critique implies that we may not help our understanding

of the social implications of Section 215 of the PATRIOT Act by identifying categories in which to home the policy. He argues that "perhaps classification is best regarded as a tool for the initial exploration and perception of pattern in complex policy data" (Rowlands, 1996, p. 20). Supporting this, Yusof, Basri and Zin's classifications cause one to consider alternative ways of construing an information policy. For example, using their categories as a starting point encourages consideration of the economic or technical dimensions of Section 215. This leads to questions regarding fair remuneration for the labours involved in granting access, or consideration of the technical measures needed to efficiently supply data to law enforcement. While Rowlands argues persuasively that classification lacks theoretical weight, there is still value in it as an exploratory strategy. That said, the classification approach fails to elucidate the interlocking political influences that contributed to the PATRIOT Act: the history of informational privacy, anti-terrorism legislation, the rapid passage of laws in the wake of September 11th, and other factors.

This thesis adopts the following definition of information policy, adapted largely from Weingarten (1989, 1996): *Information policy is the set of all formal and informal policies, rules, standards, guidelines, norms and laws that governments apply to encourage, discourage, or regulate the creation, use, storage, and communication of information.* This definition captures the formal instruments of information policy, such as laws and regulations, as well as the informal, such as policy-makers getting input and advice from consultants and private organisations. The informality element also captures the view that policy includes government *in*action as much as action (Heidenheimer, Heclo and Adams, 1990, p. 3). The definition includes standards, which are to be understood in both the informal sense, as in values and 'standard operating procedures', but also in the formal sense of technical standards and protocols, such as the SAML identity standard. A contribution of this thesis is the analysis of government-promoted technical standards as both a regulatory outcome and a 'carrier' for the institutionalisation of data protection. The above definition specifies 'governments' as the policy actor. This sets the definition apart from other sources of information policy-making, such as private organisations, and

connects it specifically to public policy. Privacy and data protection, the central issues of this research, are captured by "encourage, discourage, or regulate."

Disciplinary Ghettos

Much literature on information policy derives from the field of library science, but Rowlands (1996, p. 17) noted that disciplines as diverse as economics, law, political science, sociology, management science and policy studies are said to comprise the field. Given this mixed heritage, it is difficult to have a unifying view of what information policy *is*, or what its research focus can or should be. Doty (1998, p. 59) wrote:

> "Conflicts over the definition of information policy reveal and result from deep conflicts in the disciplinary allegiances, training, and political values of information policy analysts. Such conflicts are also based on opinions about appropriate questions, acceptable methods of inquiry, appropriate rhetorics of persuasion, realistic models of social life, acceptable modes of social behavior, the identity and relative status of stakeholders, and the role of the analyst in policy making and implementation."

Duff (2004, p. 78), citing a disciplinary list similar to Rowlands, asked, "Is it possible … to speak of information policy as having an academic identity?" To further complicate matters, formal information policies promulgated by the state have been "technology-driven" (Trauth, 1986, p. 42; Rowlands, 1996, p. 17). Policies are "piecemeal, sporadic and … reactive in the face of specific issues" (Browne, 1997a, p. 262). Braman (2009, p. 5) argued that to understand what is happening to society as a result of information policy

> "… three types of knowledge must necessarily be brought together. Research on the empirical world … [s]ocial theory … [and] [k]nowledge of current law and its history.… Historically, these diverse domains of knowledge were pursued within different disciplines that only rarely interacted.…"

This thesis answers Braman's call directly by bringing together empirical research on the emergence of unlinkability, neo-institutionalist theory, and an extensive review of relevant law and policy.

McClure and Jaeger (2008, p. 259-260) turn the problem of fragmentation on its head, arguing,

> "… information policy research is uniquely situated to draw from a vast range of approaches, sources, and disciplines. When applied properly, this array of methods can produce important insights into policy and society."

Yusof, Basri and Zin (2010, p. 210) concluded that the variety of disciplines is growing, ergo, "the study of information policy is expanding and has the potential to become a multidiscipline of its own." This thesis embraces this view and approaches the empirical data in an interdisciplinary way, using political, technical and business perspectives.

The Purpose of Information Policy

Information policy scholars debate the purpose of policy research. That debate in part is about the primacy of normative theory – a conceptualization of a preference – and empirical theory – a conception of what actually exists (McCool, 1994). That is, should information policy research be performed in service of bettering the policy-making process, or of justice and improving social conditions (Browne, 1997a; Doty, 1998; Duff, 2004)? Or, should it be neutral, value-free, and explanatory without saying what policy and policy-making should be (Rowlands, 1996; Trauth, 1986)? Turner (1997, p. 19) portrays this distinction as, "analysis *for* policy-making and *of* policy-making." Rowlands (1996, p. 16) described the latter focus as a "scientific" rationale for studying policy, and the former as "professional" or "political." He explains:

> "The scientific motivation seeks to understand policy, not to suggest what that policy ought to be. Clearly however, information policy studies undertaken for professional or political ends have a different emphasis … This approach is concerned with achieving the 'right' goal, with what policy ought to be, and therefore cannot be arrived at without reference to an ideological … or normative position. As such, it is a value-oriented approach …" (Rowlands, 1996, p. 16).

Of these two poles – the scientific and the normative – Duff (2004, p. 70) took a clear position:

> "Information policy … needs to be more clearly positioned as a normative field, one that utilizes axiological reasoning to articulate goals for the future of society … [I]t occupies a normative role in prescribing conceptions of the good information society."

Browne also agrees with the need for prescription, but in service of guiding the field's disciplinary development rather than for Duff's putative information society. She argued that a prescriptive focus "is essential … to point a direction for the development of the field of information policy" (Browne, 1997a, p. 264). Doty (1998, p. 61) also argued that the purpose of information policy research was to influence policy-making, as well as "understand social interaction" and "forge political and intellectual alliances," given its cross-disciplinary nature. McClure and Jaeger (2008, p. 258) cite both the scientific and normative purposes of information policy research, arguing for summative roles – "helping to ascertain whether the policy goals and objectives are being met" – and formative roles – "helping to continually refine and update policies" and to increase policy's "positive impact on society."

Related to the scientific/normative divide, information policy literature calls for value-critical approaches to research (Overman and Cahill, 1990; Browne 1997a, 1997b; Rowlands, 1996; Rowlands and Turner, 1997; Braman, 2002; Rowlands et al., 2002; Duff, 2004; McClure and Jaeger, 2008). Rein (1976, p. 13) writes:

> "A value-critical approach subjects goals and values to critical review, that is, values themselves become the object of analysis; they are not merely accepted as a voluntary choice of the will, unamenable to further debate."

Overman and Cahill (1990, p. 803) observed, "there is a shortage of policy research that calls attention to the countervailing trends and conflicts of values in information policy." Browne (1997b, p. 344) noted, "[v]alues in information policy have been largely neglected in information policy scholarship.…" McClure and Jaeger (2008, p. 258) stated:

> "Policy research moves beyond purely technical issues. It explains conflicts between policies and stakeholders, excoriates assumptions and values, offers guidance in articulating conflicting issues.…"

This thesis adopts Rowlands' (1996, p. 16) 'scientific' rationale; what Turner (1997, p. 19) called "analysis … *of* policy-making." It does not proffer a normative position in regards to privacy within identity management or the policy-making process. The research explores novel policy phenomena so as to better understand evolution within the policy fields of data protection and identity management, and to define identity management as an emerging sub-field of information policy. As will be shown below, the new institutionalist approach can be used to address the above criticisms of policy research. It can subject the values underpinning unlinkability choices to critical analysis so as to articulate the norms informing policy choices.

Theoretical Weaknesses of Information Policy

One frequent point of agreement in assessments of information policy research is its under-theorised character (Overhill and Cahill, 1990; Rowlands, 1996; Browne, 1997a, 1997b; Doty, 1998; Agre, 2003; Bjorck, 2004; Duff, 2004; Braman, 2009). Overhill and Cahill (1990, p. 803) wrote:

> "From a theoretical perspective, the problem [of coordinated policy development] is one of understanding the values and normative structure that shape that shape the information policy debate. Most approaches to information policy have understated the role of values and normative structures."

Rowlands (1996, p. 13) highlighted the "relatively scant attention … paid to the theoretical foundations of the subject." Browne called for ways to "ensure that the field is based on defensible ontological and epistemological foundations" (1997a, p. 264) in order "to form a unique interdisciplinary field which builds on the theoretical foundations of both information studies and policy studies …" (1997b, p. 340). Duff (2004, p. 69-70) wrote, "in both theory and practice, information policy has not yet reached any kind of satisfying plateau."

These theoretical weaknesses and the highly heterogeneous nature of information policy frustrate systematic analysis. Trauth (1986, p. 41) called for an "integrative approach to information policy research." She described the

history of US information policy as being tied to developments of particular kinds of information processing technology, rendering policies sectoral and fragmented. This causes related policy research to be "discipline-bounded" (Trauth, 1986, p. 42). Citing technology convergence, a growing dependence on information and its value as a societal resource, Trauth argued for change in information policy analysis; an interdisciplinary and integrative approach. To do so, she identified

> "… the set of activities comprising [US] information policy. What comes immediately to mind is the set of existing laws. However, information practices are influenced by other forces as well: economic, societal and international. In addition to establishing the component parts, the interactions among them must also be examined. Further it is by extrapolating from specific policy contexts that we can make general observations about US policy. Thus, this research needs to examine the component interactions not only within, but between policy contexts." (1986, p. 43)

In addition to this cross-contextual analysis, Trauth (1986, p. 43) argued that "policy research should make note of the philosophies underlying such policy and the extent to which they are consistently reflected." Rowlands (1996) discussed in detail the fragmentation within information policy studies, and repeated Trauth's assertion that research has been discipline-bounded. He argued that "[t]he fragmentation of information policy research is mirrored by a fragmentation of policy-making institutions" (Rowlands, 1996, p. 17). Browne (1997a, p. 262) reiterated this view:

> "… responsibility for different, and often overlapping, aspects of information policy has been based across different government departments in developed countries. Overarching frameworks which can be used to integrate policy at a broad conceptual level and in a coherent fashion are notably absent."

Accordingly, several authors cite the need for theoretical and methodological pluralism (Trauth, 1986; Braman, 1989; Rowlands, 1996; Browne, 1997a, 1997b; Doty, 1998; Duff, 2004; Galperin, 2004; McClure and Jaeger, 2008). The reasons cited are to achieve greater coherence in analysis, to advance the field, and to improve policy-making. Braman (1989, p. 233) wrote:

> "Theoretical pluralism seems an appropriate way to think about phenomena that occur and processes that unfold in different ways at different levels of a highly articulated social structure."

In recent work, Braman (2009, p. 5) noted that failure to bring together empirical work, social theory and knowledge of law and its history "cripples policy-making." Information policy research lends itself to multiple methods of data collection and analysis, helping to optimize data collection and allow for better analysis (McClure and Jaeger, 2008, p. 259).

Rowlands (1996, p. 20) noted that "information policy exists at two layers: that which is *explicit* and recorded in documentary form, and that which is expressed *implicitly* in the form of habits, received wisdoms, unwritten codes of behaviour, expectations and societal norms." Browne (1997b, p. 342) wrote: "the newer approaches to understanding phenomena are critical for information policy, given their capacity to show events through the eyes of the actors in situations within a public world of norms, conventions and rules." Trauth (1986, p. 41) stated:

> "US policy has evolved in a decentralized fashion. The resulting national policy is implicit in nature, consisting of a collection of laws, precedents, expectations, and societal norms."

This focus on the normative aspect of information policy is seen in a host of publications (Overman and Cahill, 1990; Weingarten, 1996; Meijer, 2003; Braman, 2004; Duff, 2004; Galperin, 2004; Adams, Murata and Orito, 2010; Mueller and Lentz, 2010).

In summary, information policy is an under-theorised, decentralised, heterogeneous policy domain. Information policies encompass laws, rules, norms, expectations, cultural elements, formal and informal practices, the explicit and the implicit. While there is an ongoing debate as to the purpose of information policy research, there are strong arguments to examine that research for its underlying value assumptions. The above qualities steer research in the direction of social theories that can encompass these characteristics so as to explain policy development and change. This thesis

embraces the arguments for greater theoretical engagement within information policy research. It acknowledges the interplay of the formal and the informal, norms, values and culture within information policy-making. The next section specifies the disciplinary sub-topics of this thesis: identity management, data protection and e-government. The remainder of the chapter explores new institutionalism as an approach to theoretically enrich the research.

Information Policy Sub-topics

The empirical research of this thesis concerns unlinkability within identity management, data protection, and e-government, all of which are part of the multidiscipline of information policy. Identity management encompasses the creation, maintenance, alteration and revocation of electronic identity credentials and attributes. A European Commission research report succinctly states:

> "One crucial question lies at the heart of digital identity management: how do I know you are who you say you are?" (Stevens et al., 2010, p. 1)

Data protection includes a wide variety of issues related to the creation, processing, privacy, use, storage and transmission of personal data. E-government is the use of electronic technologies by government to accomplish its business with the private sector, with citizens and internally; it denotes the use and transmission of digital data. Unlinkability is a characteristic of identity management systems where the online activities of an individual are intentionally obfuscated by breaking the 'links' created as she goes from site to site. All of the above terms and concepts are examined in Chapter 4.

A government's choice to build unlinkability into its identity management system is an information policy choice that is both influenced by and part of its data protection regime. Taken together, all of the choices related to the creation and management of electronic identities can be said to be a country's 'identity management policy.' If electronic identities are used with government websites and other resources, then its identity management policy interacts with its e-

government policy. All of these policies form part of a country's information policy.

There is limited discussion in information policy literature about the existence or boundaries of national identity management policy (Davies and Hosein, 2007; Whitley and Hosein, 2009). A core contribution of this research is the definition of this sub-field of information policy: *Identity management policy is the set of laws and policies enacted by governments and supranational bodies concerning the facilitation, procurement, use, liability, legal nature, interoperability, technologies, risk methodologies, lifecycle and privacy of digital identities for its citizens and employees. This includes physical and logical authentication, e-signature, and electronic identification technologies for access to physical and electronic resources.* The empirical data chapters (5 and 6) and policy comparison chapter (7) supply necessary data and analysis to validate this definition.

By studying the intersection of privacy, data protection, national citizen identification initiatives and e-government, this thesis enriches understanding of the relationship between policy actors, values, technology and policy-making in the field of identity management. A definition of identity management policy and an exploration of its institutional dynamics broaden the field of information policy.

Theoretical Approach

In line with the information policy scholarship cited above and its calls for integrative and interdisciplinary approaches to information policy research, the new institutionalist theoretical approach is used to frame and analyse the collected empirical data on the emergence of unlinkability. As will be explained below, a new institutionalist, or neo-institutionalist, approach addresses the institutional dimension of policy-making, examining the formal rules underpinning a policy domain, norms, values, and implicit and informal rules. This approach analyses the actors within policy-making – such as legislatures, interest groups, bureaucracies, the subjects of policies,

organisations and citizens – and the institutional landscape in which they are embedded. It facilitates the analysis of actors' values and how their choices are influenced by norms, cultural beliefs, cognitive scripts, narratives, institutional structure and past decisions. New institutionalism is not discipline-bounded – political science, economics, organisational studies and sociology all use and contribute to its theoretical development. It encompasses a wide range of methodologies and data collection techniques, and subjects the values of institutional actors to examination (Lowndes and Roberts, 2013). These characteristics address many of the criticisms of information policy research outlined above.

One research question of this thesis is: How is unlinkability emerging as public policy? A neo-institutionalist approach would analyse the institutions involved in such a policy choice:

> "… institutions are the variable that explain political life in the most direct and parsimonious manner, and they are also the factors that themselves require explanation." (Lowndes and Roberts, 2013, p. 6)

The remainder of this chapter will show how an analysis of the institutions involved in identity management policy-making helps to explain the policy development of unlinkability. This analysis highlights formal instruments, informal practices, relationships and artefacts – the 'carriers' of institutionalisation (Scott, 2003) – and how different actors enact the institution of data protection, which powerfully influenced identity management policies.

Several scholars have applied an institutionalist approach to information policy issues. Bellamy and Taylor (1996; see also Bellamy and Taylor, 1998) examined the institutional dynamics of computerisation in the UK criminal justice system. They use a case study of a UK government project to coordinate informational resources within the criminal justice system as a way to illustrate mechanisms of change and barriers to change in government (1996, pp. 51-52). Bellamy and Taylor conceive of an 'information polity' – a "normative, cognitive and symbolic order" (1996, p. 56) of information resources amongst a set of political institutions; in this case, the departments of the criminal

justice system. They illustrate how the institutional dynamics of power, organisational boundaries, the structuring of information and rationalising discourses shape the political environment in which attempts at government change occur. Bellamy and Taylor show how the tension between actors and political change programmes can be usefully examined through analysis of symbols, methods of legitimating agency structures, political agendas and historical context.

Robbin (2000) examined the rules and practices of the political institutions involved in US government decisions about how to classify population data, considering theories of the role of the state and the social construction of identity. She used a case study of the revision of a US national standard of categories on 'race' and 'ethnicity' to illustrate the role of political institutions in the shaping of social identities and preferences. Robbin showed how the prior institutionalisation of these categories became destabilised by interest groups and conflicting discourses, leading to minor revisions in the standard. The revision was contested because the categories were tied to political and material benefits for disenfranchised groups, such as American Indians. They were also powerful symbols that influenced the ways that category members self-identified. The categories were given weight by their state origins, and as informational boundaries they influenced a variety of other institutions. Robbins' work illustrates the institutional power of vocabularies (Meyer and Rowan, 1977) in defining political choices.

Agre (2003) examined how digital libraries are embedded in their institutional environments so as to encourage designers of such libraries towards appropriate and practicable designs. He posited that digital libraries are both machines and institutions; both a database and an extension of the institution of libraries. Society, Agre wrote, "will evaluate digital libraries in terms of the ways that they fit, or fail to fit, into the institutional world around them" (p. 219). He pointed out that libraries interact with a wide variety of other institutional domains, such as scholarship, law and the professions. Such diverse interaction poses challenges for designers of digital libraries, who must

balance the orientations of a home institution of libraries with the other institutions it interacts with.

Meijer (2003) analysed how institutional safeguards, separate from technological and organisational ones, led actors to trust the authenticity of digital public records. He examined eleven different Dutch cases where the authenticity of records was critical to accountability in public administration. In eight of the cases, either technical or organisational safeguards were used to ensure the records' authenticity. In the three remaining cases, there were neither technical nor organisational safeguards, but the authenticity was not questioned. Meijer argued that an institutional safeguard was relied upon: the belief that public servants would behave lawfully and appropriately with regard to recordkeeping.

Björck (2004) argued for new institutionalist theory to be used in information technology security research. Finding research in this area to be largely atheoretical, he cites institutional scholarship in general information systems research to show how institutional concepts might be used in security research. He proposed that institutionalism could help explain why formal security and actual security behaviours differ, why organisations create and maintain formal security structures without fully implementing them, and what mechanisms are actually controlling security behaviour.

Galperin (2004) explains the differences between the UK's and US's digital television spectrum policies through an explicitly new institutionalist analysis. To explain political outcomes in communications policy research, he contrasts theories of interest groups, the role of ideas, and technological change, finding them inadequate to explain outcomes. He uses institutional analysis to examine the power relationships and political structures that underpinned the giveaway of digital television spectrum licenses to incumbent broadcasters. The analysis shows that the broadcasters won the day because members of Congress relied upon close relations with local broadcasters to help win their elections. It was not only the actions of powerful national interests that caused a political

choice, but also a self-interested action by policy-makers who needed favourable local news coverage from local broadcasters

Aichholzer and Strauβ (2010) applied actor-centered institutionalism to their investigation of identity management systems in Austria. They explain the system innovation of the national IDM system for citizens by considering the various political actors involved and institutional features, such as the lack of a requirement for Austrians to possess an identity document. Citing e-government as the main driver of the IDM system, Aichholzer and Strauβ explain that e-government stakeholders took a preeminent role in the constellation of actors influencing the system design.

Kim, Kim and Lee (2009) explained the success of a local Korean e-government platform and the adoption of it as a model for national use through institutionalist analysis. The platform, known as OPEN, was deployed both to increase administrative transparency and reduce corruption. The authors show how three institutional mechanisms – regulatory/coercive, cognitive/mimetic and normative – acted to create the e-government platform, reinforce its use in Korean society, and diffuse it to a national scale.

While there is literature that uses neo-institutionalism within information policy research, and some of it deals directly with data protection issues, there is little discussion of treating data protection *as* an institution. Burkert (1981) examined the institutions of data protection, but from a purely functional perspective. His goal was to problematise the role of data protection authorities *vis-à-vis* European data protection laws. Adams, Murata and Orito (2010) examined legal, economic, technological and cultural factors in the adoption of Japan's data protection regime. They admitted that their arguments are not a rigorous use of institutionalism, but rather that some evidence of path dependence appears in the background pressures leading to the adoption of Japanese data protection rules (2010, p. 98). Righettini (2011) explicitly used new institutionalist analysis in a comparison of the regulative policies of French and Italian data protection authorities. Her work is an excellent analysis

of the relationship among institutional actors, networks, norms, and narratives leading to the choice of regulative instruments and "style" (2011, p. 162). These works consider institutional effects and actors that influence data protection, and they focus on the institutions *of* data protection – authorities – and factors leading to the creation of data protection instruments. They do not, though, discuss data protection as an institution in and of itself.

Following the explanation of new institutionalism below, this chapter conceptualises data protection an institution, defined here by March and Olsen (2004, p. 5, orig. emph.):

> "An institution is a relatively stable collection of rules and practices, embedded in structures of *resources* that make action possible – organizational, financial and staff capabilities, and structures of *meaning* that explain and justify behavior – roles, identities and belongings, common purposes, and causal and normative beliefs."

The remainder of the chapter is dedicated to explaining new institutionalism, how data protection is an institution, and the utility of new institutionalism in explaining the policy development of unlinkability.

The 'Old Institutionalism'

Most political science in the first half of the 20th century is characterised by a study of formal institutions: constitutions, legal systems, government structures and economic organizations (Shepsle, 1989; Scott, 2008; Lowndes, 2010). "Institutionalism *was* political science" (Lowndes, 2010, p. 60). This early institutionalist orientation yielded intricate descriptions of rules, rights, procedures and structures, with limited attention paid to any notions of change (Scott, 2008, p. 6). Further, "the tone of these studies was more that associated with moral philosophy and less that of empirical science." (Scott, 2008, p. 6) This focus on formal institutions and normativity was rejected by the behavioralism movement in political science and rational choice economics which saw those institutions and political outcomes as the "aggregation of individual actions" (Shepsle, 1989, p. 133; Scott, 2008, p. 7). These actions, it was argued, arose from sociological and psychological principles and

preferences to maximise self-interest, respectively. The two movements eschewed the normative, prescriptive approaches of earlier scholars, and devoted their attentions to the primacy of the individual actor over the internal workings of political structures (Scott, 2008, pp. 7-8).

Modern conceptions of institutions within sociology are evident from the end of the 19th century onwards. The binding power of norms and their transmission via groups of people appear in the scholarship of Spencer, Sumner, Cooley and Hughes in the first half of the 20th century (Scott, 2008, pp. 8-11). Belief systems, symbols and cultural rules are seen to govern social behaviour in the work of Durkheim and Weber (Scott, 2008, pp. 11-15). In the 1960s, Berger and Luckmann emphasised the 'social construction of reality,' and the role of cognitive frameworks in shaping behaviour (Scott, 2008, pp. 15-16).

Institutionalist thinking appears within the study of organisations in the 1950s (Scott, 2008, pp. 20-23). This work highlighted how values, rituals and symbols influenced actors. Organisations came to be seen as analytically separate from institutions. Within organisational theory, the dominant perspective in the late 1970s was of organisations adapting (or attempting to do so) to their environment to secure an appropriate fit within the confines of 'bounded rationality' – the set of rational choices perceived to be available given the limitations of awareness, information and time (Greenwood, Oliver, Sahlin, and Suddaby, 2008, p. 3).

The New Institutionalism

From the late 1970s onwards, scholars became disenchanted with the atomistic, "undersocialized conceptions of human action" (Granovetter, 1985, p. 483; DiMaggio and Powell, 1991). In 1984, March and Olsen coined the term 'new institutionalism' in recognition of a resurgent interest in institutions and their power to explain and understand society. Rather than seeing political phenomena as the aggregate consequences of individual behaviour, new institutionalist scholarship asserted that political institutions play a more

autonomous role in shaping outcomes (Lowndes, 2010, p. 63); that political life is organised around rituals, ceremonies and symbols; that political experiences shape and are shaped by peoples' preferences, rather than those preferences being exogenous; that institutions affect power distribution, which in turn affects the institutional landscape; that culture has a role in shaping organisational reality (DiMaggio and Powell, 1991, p. 12). March and Olsen (1984, p. 735) rejected prior political science scholarship that saw politics as "epiphenomena" – phenomena that arise secondarily from other phenomena – affected by conditions such as class, geography, ethnicity, language, economic conditions and culture, but not affecting them. They disagreed that social systems could be ultimately described and explained by the actions of individuals and their calculated, deliberate decisions. March and Olsen (1984) drew attention to the omnipresence of myth, symbols, ritual and ceremonies in political and social life. They noted that the political science of their day reduced these elements to mere strategic manoeuvring by actors – "window-dressing for the real political processes, or as instruments by which the clever and the powerful exploit the naïve and the weak" (1984, p. 738). Instead, the new institutionalism they posited treated symbols and ritual as core phenomena that could explain behaviour and outcomes. Meyer and Rowan (1977) asserted that myths and ceremonies, rather than formal structures of coordination and control, are the critical dimensions of how organisations function. Further, they argued that organizations become isomorphic – tending towards structural and behavioural similarity – with other organisations in their institutional environment because of interdependencies that occur between them, so as to enhance legitimacy, and to better survive.

Admittedly, the new institutionalism was and is not necessarily consistent or coherent. A dozen years after March and Olsen (1984) noted this, Hall and Taylor wrote, "it does not constitute a unified body of thought" (1996, p. 5). Partly, this is because of the tension caused by two potentially irreconcilable views: rationally coherent behaviour of actors maximizing their utility versus sociological conceptions of preferences and behaviours shaped by the actors' institutional landscape (March and Olsen, 1984; Lowndes, 2010). Further,

there is disagreement as to whether or not institutions yield efficient outcomes (Meyer and Rowan, 1977; Shepsle, 1989). Different scholars focus on different kinds of institutions, defining exactly what an institution is in limited or more expansive terms. There are many institutionalisms, DiMaggio and Powell (1991, p. 1) noted, and "it is often easier to gain agreement about what [the new institutionalism] is *not* than about what it *is*."

The Variants

There are several variants of new institutional approaches (Lowndes, 1996; Hall and Taylor, 1996; Hay and Wincott, 1998; Lowndes, 2010). Initially, three were identified: rational choice, historical, and sociological. Through the 1990s and 2000s, additional variants were postulated and named, including normative, empirical, network and constructivist (Lowndes, 2010). Lowndes (2010, p. 64-66) and Hall and Taylor (1996, p. 7) have pointed to two 'poles' of the spectrum of approaches: rational choice or 'calculus' on one end, and normative or 'cultural' on the other. All of the variants exist between these two poles. The initial three variants are the 'main strands' of institutionalism (Lowndes and Roberts, 2013, p. 32).

Rational choice institutionalism is derived largely from the field of economics, arguing that individuals create political institutions to maximise their self-interest ('utility'), stabilise relationships and reduce the transaction costs between people, groups and organisations (Koelble, 1995). Preferences (in favour of utility maximisation) are seen as exogenous, not influenced by institutions, although institutions "define the choice set" (North, 1991, p. 97). Rational choice theorists frame institutions as solutions to collective action dilemmas, providing reasons and ways for individuals to act in a concerted way. Institutions rely, in part, on enforcement (e.g., penalties) in order to be robust (Levi, 1990; North, 1991). Rational choice theorists tend to emphasise institutions' durability. This durability arises in part because the transaction costs of alternative institutions are too high to allow change (Shepsle, 1989, p. 144) or because entrenched players are incentivised to maintain current institutional structures (North, 1990, p. 99).

Sociological institutionalists argue that institutions shape and are shaped by norms and values, interests, identities and beliefs. In contrast with rational choice, individuals' preferences are seen to be influenced by institutional arrangements and power dynamics; people's behaviour is not strategic, but bounded by a worldview influenced by institutions (Hall and Taylor, 1996). Meyer and Rowan (1977) argued that institutions persist and thrive by their actors' adherence to myths, ceremonies and rituals that validate the rationality of the rules those myths and rituals promote. Deviation from these myths and rituals threatens the perceived legitimacy of organisations. Institutions both adapt to and shape their environment, and more powerful actors attempt to build their goals and processes directly into society as institutional rules. Meyer and Rowan (1977) also speak of the importance of organisational language and vocabularies of structure as specific means of legitimating actors' activities. In this way, and by aligning internal goals with externally defined worth, organisations improve their appearance of legitimacy and thereby their survival. They note the potential for conflict from inconsistent myths co-existing within institutional environments, and point out that efficiency is often less important than adherence to rituals and rules. Greenwood, et al. (2008), in contrast with rational choice conceptions of institutions, disregard overt enforcement as a defining characteristic, and see institutionalisation in simple actions between individuals, such as a handshake. In regards to organisations, they summarise the process of institutionalisation in three mechanisms: *coercive*, where external constituents encourage or force institutional elements to be absorbed; *normative*, where actors adopt local norms and obligations; and *mimetic*, where organisations copy others so as to seem legitimate, or not seem deviant (see also DiMaggio and Powell, 1983).

Historical institutionalism sees the institutional organisation of a polity as the principal factor in generating distinctive policy outcomes (Hall, 1996). Giving primacy to political institutions over economic and cultural ones, historical institutionalists highlight power asymmetries inherent in and affected by changes within institutional arrangements. These asymmetries influence the

decision-making processes that create policy. Historical institutionalism highlights the stable nature of institutions, noting that social forces and prior policy choices and institutional arrangements may engender 'path dependency.' That is, historical events lay down paths that shape future outcomes, versus the view that similar forces in different contexts would produce similar results. Accordingly, historical institutionalism is often used to compare policies in different countries. Important to these comparisons is the concept of "sequencing" (Thelen, 1999, p. 388; Weir, 1992, p. 192). The sequence – i.e., the timing – of events and interactions between political processes and institutional development must be considered to illuminate path dependency and analyse policy outcomes. And, given the influence of past choices, institutions are acknowledged to suffer from and cause unintended consequences, resulting in inefficiency. Path dependency arises from 'feedback mechanisms,' including 'coordination effects,' where, "once a set of institutions is in place, actors adapt their strategies in ways that reflect but also reinforce the 'logic' of the system" (Thelen, 1999, p. 392).
The other feedback mechanism is the:

> "… distributional effects of institutions. The idea is that institutions are not neutral coordinating mechanisms, but in fact reflect, and also reproduce and magnify, particular patterns of power distribution in politics … facilitating the organization and empowerment of certain groups while actively disarticulating and marginalizing others." (Thelen, 1999, p. 392)

Policy choices can thereby be constrained as past decisions restrict future possibilities.

Like its sociological variant, historical institutionalism sees institutions as shaping ideas and interests, which influence the goals of political action (Koelble, 1995, p. 239). Those goals and resultant actor choices, in turn, influence institutional arrangements. Powerful actors seek to embed rules into institutional arrangements that favour their desired outcomes. Path dependency, however, can result in limitations on future policy-making, what Margaret Weir calls "bounded innovation" (1992). Further, historical institutionalists give credence to non-institutional factors in political outcomes, such as

economic structures and the diffusion of ideas. Proponents and commentators on historical institutionalism point out that such analysis does not represent an all-encompassing evaluation of the causes of political outcomes (Thelen and Steinmo, 1992, p. 13).

A Holistic Approach to Institutional Analysis

Information policy scholarship calls for integrative approaches to research, arguing for the necessity of analysing norms, mores, rules and informal influences alongside the formal products of legislatures, courts and administrations. To achieve this value-critical approach that examines the implicit as well as the explicit, each of the three institutionalist variants can contribute. Given the rich variety of empirical evidence and potent range of analytical approaches, a holistic evaluation would be most constructive. Rather than declaring for one branch of institutionalism or another, an 'omnibus' conception of institutions and their dynamic processes will offer a fruitful analysis of the data under study. Scott (2003, p. 881) observes that "it is important to recognize that most full-fledged institutions are made up of diverse elements. There are few 'pure' cases." Historical institutionalism's focus on political institutions, process tracing, the foreclosure of policy choices due to prior choices, and comparative studies makes it particularly valuable for this research. And, while German and US information policy can be usefully analysed from the perspective of timing, sequence and history, there are also traces of cultural scripts, leading one to include a sociological institutionalist perspective as well. Commercial actors pursuing their own self-interested ends are usefully examined with a rational choice perspective.

This study will adopt Lowndes' (2010), Lowndes and Roberts (2013) and Scott's (2008) holistic approach, which opens up institutional theory as a pluralistic framework that has particular utility for addressing gaps in information policy research. This will align the analysis with calls in information policy research for inclusiveness and theoretical pluralism. The next sections synthesise the various strands of institutionalist thought into a holistic approach.

The Core Propositions of Institutionalism

In a synthetic appraisal of its various camps, Lowndes (2010, pp. 66-71) describes the evolution of 'old' to new institutionalism as movement along six "analytic continua":

> (a) *"From a focus on organizations to a focus on rules."* Institutions are seen as rule sets rather than organisations themselves. For example, instead of a focus on specific government agencies, new institutionalists would be more likely to study the procedures that guide and constrain them. Organisations become both the actors subject to institutional constraints, and arenas in which those rules and constraints are developed and expressed.
> (b) *"From a formal to an informal conception of institutions."* Informal rules and unwritten conventions are seen to be as important as formal arrangements and mechanisms; formal and informal rules may influence and support one another.
> (c) *"From a static to a dynamic conception of institutions."* New institutionalists explicate the stability and change processes of institutions, recognizing that, as rules and processes rather than things, they must be sustained or changed through human action.
> (d) *"From submerged values to a value-critical stance."* New institutionalism attempts to identify the ways that institutions embody values, and how institutions may cultivate values. There is a recognition that political values shape power relationships, and must therefore be analysed to understand how the institutional landscape is formed.
> (e) *"From a holistic to a differentiated conception of institutions."* Rather than focusing on systems of government, new institutionalists focus on component institutions of political life: e.g., decision-making systems, contracting rules, budgetary arrangements, and tax systems. Institutions preserve and embody differential power resources, privileging some and disenfranchising others. And, institutions exist and adapt within a diverse environment, producing variation and deviation.
> (f) *"From independence to embeddedness."* Institutions exist within a plurality of rules and contexts; they are nested within other rules and regimes. Some writers see institutional choices made early in policy processes as delimiting future choices, causing those institutional structures to become embedded. Some policy development paths are foreclosed, while others are not.

This final point is summarised by Powell (1991, p. 188):

> "The critical agenda for institutional analysis should be to show how choices made at one point in time create institutions that generate recognisable patterns of constraints and opportunities at a later point."

Most important to the present research are (a), (b), (d) and (f). The institution of data protection is best viewed as rules and procedures. Taken together, they constrain and enable actors and technology. Those actors and that technology then, in turn, enact and affect the institution of data protection. Understanding how unlinkability emerged requires attendance to the informal and normative features of policy-making. The values of relevant actors must be critically appraised to understand how those values influenced policy development. Data protection, identity management, national identification and other policy contexts overlap with one another; unlinkability cannot be explained without analysing the interdependencies of its policy milieu.

Lowndes' treatment pulls together various analytical pathways of institutionalist thought, enabling further synthesis that can be applied to the empirical data. The next sections define institutions, and introduce Scott's framework to collapse the various institutionalisms into a synthetic analytical approach.

Various Definitions of Institutions

The core features of an institution are shared across all of the different camps: institutions are rule-like and impersonal; they are, in part, comprised of norms; they have stabilising effects, allowing actors to make choices in the absence of information they might use to make decisions (rational choice), or by encouraging people to behave in line with established cultural practices or cognitive scripts (sociological); they affect and are affected by their environments; they tend to be stable, though are subject to change, competition and destruction. However, there is dissent, or at least a different focus, along the purported spectrum of rational choice to normative. The former sees behaviour as driven by rationality (however bounded) in favour of utility maximisation. The latter explains behaviour as deriving from a "logic of appropriateness" (March and Olsen, 2004); as a result of 'satisficing' (settling for the best sub-optimal choice available) (Simon, 1955); as a result of being unable to conceive of alternatives, or a belief that alternative choices are

unrealistic (DiMaggio and Powell, 1991). Rational choice sees institutions as the product of conscious human design, whereas the normative viewpoint disavows conscious design.

In general, there is a taken-for-granted quality to institutions, as well as repetition and formal and informal constraints (Greenwood, et al., 2008). Offe (2006, p. 16) writes of institutions having codes of conduct and "sector-specific ethos" – this comports with new institutionalism in general, as does his view that institutions subsume and subordinate individuals. Depending on the author, institutions can be seen as organisations themselves, such as the US Congress (Shepsle, 1989), formal rules, such as those of electoral systems (Thelen and Steinmo, 1992) and constitutions (North, 1991), and macrosocial conditions, such as sovereign statehood (DiMaggio and Powell, 1991). Broader yet is Friedland and Alford's (1991, p. 249) conception of institutions:

> "The central institutions of contemporary Western societies – capitalism, family, bureaucratic state, democracy, and Christianity – are simultaneously symbol systems and material practices."

This issue of 'material practices' is important to the cases under study, and will be discussed further below.

In an explicit attempt to bring "some order into the discussion," Scott (2008, pp. 47-48) proposed the following omnibus conception of institutions:

> "Institutions are comprised of regulative, normative and cultural-cognitive elements that, together with associated activities and resources, provide stability and meaning to social life…. In this conception, institutions are multi-faceted, durable social structures made up of symbolic elements, social activities, and material resources." (see also Scott, 2003, p. 880)

This broad definition, encompassing the symbolic, the social and the material, captures a wide swathe of institutionalist thought. It provides a foundation on which to analyse the empirical data of this thesis, which exhibits all three dimensions. The next section expands upon Scott's synthesis.

Synthesis of Institutionalisms

Scott (1995; 2003; 2008) draws together the various strands of new institutionalist scholarship and finds three key emphases that he terms the 'three pillars' of institutions: regulative, normative and cultural-cognitive.

> "These elements are the central building blocks of institutional structures, providing the elastic fibers that guide behavior and resist change." (Scott, 2008, p. 49)

One or all of these pillars appear across the various conceptions of institutions, with different scholars weighting one or the other as central (Scott, 1995, p. 34-35). Scott (1995, p. 35; 2008, p. 51) writes:

> "By employing a more analytical approach to these arguments, we can identify important underlying theoretical fault lines that transect the domain."

Scott (2008, p. 51) explained the three pillars in the following figure:

Figure 2.1 Three pillars of institutions

	Regulative	*Normative*	*Cultural-Cognitive*
Basis of compliance	Expedience	Social obligation	Taken-for-grantedness Shared understanding
Basis of order	Regulative rules	Binding expectation	Constitutive schema
Mechanisms	Coercive	Normative	Mimetic
Logic	Instrumentality	Appropriateness	Orthodoxy
Indicators	Rules Laws Sanctions	Certification Accreditation	Common beliefs Shared logics of action Isomorphism
Affect	Fear Guilt / Innocence	Shame / Honor	Certainty / Confusion
Basis of legitimacy	Legally sanctioned	Morally governed	Comprehensible Recognizable Culturally supported

Source: Scott, 2008, p. 51

Scott further writes:

> "The three elements form a continuum moving 'from the conscious to the unconscious, from the legally enforced to the taken for granted.'" (2008, p. 50, quoting Hoffman)

The regulative pillar concerns explicit regulative processes: "the capacity to establish rules, inspect or review others' conformity to them, and as necessary, manipulate sanctions – rewards or punishments – in an attempt to influence future behavior" (Scott, 2008, p. 52). These processes may be formal, such as via police or judicial actions, or informal, such as shaming. Scott (2008, p. 53) explained:

> "Force, sanctions, and expedience responses are central ingredients of the regulative pillar, but they are tempered by the existence of rules, whether in the guise of informal mores or formal rules and laws."

The primary mechanism of control, in the language of DiMaggio and Powell (1983, p. 150) is coercion (Scott, 2008, p. 52). This coercive power can commonly originate with states as an 'enforcer' via surveillance and sanctioning. However, it is also seen in inducements and with other actors, such as favourable pricing by private firms to select groups (Scott, 2008, p. 53).

The normative pillar emphasises "normative rules that introduce a prescriptive, evaluative, and obligatory dimension into social life. Normative systems include both values and norms" (Scott, 2008, p. 54). Values are conceptions of the desirable or the preferred, including standards by which to compare and assess existing structures and behaviours (Scott, 2008, p. 54). Norms define how things should be done; how to legitimately pursue valued ends. Normative systems define goals and the appropriate way to pursue them (Scott, 2008, p. 54-55). Specialised values and norms that apply only to specific social positions or particular individuals are called 'roles'. Roles are normative expectations held by actors in a situation, experienced as both an internal and external force (Scott, 2008, p. 55). Scott explained:

> "The normative approach to institutions emphasizes how values and normative frameworks structure choices. Rational action is always grounded in social context that specifies appropriate means to particular

> ends; action acquires its very reasonableness in terms of these social rules and guidelines for behavior." (Scott, 1995, p. 38)

The basis of compliance of normative institutional elements is the force of mutually reinforcing obligations.

The cultural-cognitive pillar concerns "the centrality of cultural-cognitive elements of institutions: the shared conceptions that constitute the nature of reality and the frames through which meaning is made" (Scott, 2008, p. 57). This pillar gives primacy to symbolic systems and cultural rules, and their preservation and modification through human behaviour. Of foremost importance are constitutive rules that involve the creation of categories, typifications, and the social construction of actors and roles. Scott uses American football as an example: the rules constituting the game create "the goalposts and [field layout], ideas such as winning and sportsmanship, and events such as first downs and offsides," as well as the players, coaches and referees (Scott, 1995, p. 41-42). These constitutive rules are fundamental to social life, manifesting in basic concepts such as citizens, employer/employee, and families. The rules construct not only individual actors, like people, but also collective entities, such as firms and organizations and states. Moreover, the social construction of actors resulting from these rules defines what the actors see as their interests: political parties seek votes, firms pursue profits, Ph.D. students seek to submit and pass their theses. The basis of compliance of cultural-cognitive structures is their taken-for-granted qualities; other types of behaviour may be literally inconceivable (Scott, 2008, p. 58).

Jepperson (1991) calls institutionalisation a "particular set of social reproductive processes" (p. 145), "a property of an order" (p. 147), "a particular state, or property, of a social pattern" (p. 149). He speaks of three primary 'carriers' of institutionalization: culture, regimes and formal institutions (1991, p. 150-151). Regimes are

> "… explicitly codified rules and sanctions – without primary embodiment in a formal organizational apparatus. A legal or constitutional system can operate as a regime in this sense, but so can,

> for example, a profession (or for that matter, a criminal syndicate)." (Jepperson, 1991, p. 150)

Monitoring and sanctioning are expected to come from some kind of differentiated or central authority. Culture is "those rules, procedures, and goals without primary representation in formal organization, and without sanctioning by some 'central' authority" (Jepperson, 1991, p. 151). Scott (2008, p. 79-85) adapted Jepperson's concept of carriers, stating that institutions are carried by symbolic systems, relational systems, routines and artefacts. Institutions are 'conveyed' upon these carriers:

> "They point to a set of fundamental mechanisms that allow us to account for how ideas move through space and time, and who or what is transporting them." (Scott, 2008, p. 79)

The relationship between the three pillars and carriers is summarized by Figure 2.2

Figure 2.2 Institutional pillars and carriers

	Pillar		
	Regulative	*Normative*	*Cultural-Cognitive*
Symbolic systems	Rules Laws	Values Expectations	Categories Typifications Schema
Relational systems	Governance systems Power systems	Regimes Authority systems	Structural isomorphism Identities
Routines	Protocols Standard operating procedures	Jobs Roles Obedience to duty	Scripts
Artifacts	Objects complying with mandated specifications	Objects meeting conventions, standards	Objects possessing symbolic value

Source: Scott, 2008, p. 79

The entries in the table in Figure 2.2 "describe the content of the message – what is being transported" (Scott, 2008, p. 80).

With regard to symbolic systems,

> "… the symbols of interest include the full range of rules, values and norms, classifications, representations, frames, schemas, prototypes, and scripts used to guide behavior." (Scott, 2008, p. 80)

The symbol emphasised varies depending on which element (pillar) of institutions is accorded prominence. Symbolic systems code and convey information. In relation to the empirical data under study, the institution of data protection is carried in part by laws (regulative) and by expectations that society should take steps to ensure some measure of privacy of personal data (normative).

Relational systems are "made up of connections among actors, including both individual and collective actors" (Scott, 2003, p. 886). They rely "on patterned interactions connected to networks of social positions…" (Scott, 2008, p. 81). In this category of carrier we find, for example, professional groups, ties within and among organisations, and communities of practice.

Routines "are carriers that reflect the tacit knowledge of actors – deeply ingrained habits and procedures based on inarticulated knowledge and beliefs" (Scott, 2008, p. 82). Routines are "repetitive patterns of activity" (Scott, 2008, p. 83, quoting Winter) learned within organisations and often sustained by relational systems. They are habitualised behaviours and tacit knowledge.

An artefact is "a discrete material object, consciously produced or transformed by human activity, under the influence of the physical and/or cultural environment" (Suchman, 2003, p. 93). It is created "to assist in the performance of tasks" (Scott, 2003, p. 882). Artefacts embody "both technical and symbolic elements" (Suchman, 2003, p. 99). Within information policy research, the institutional consideration of artefacts is a neglected subject. This research broadens such research by examining the institutional effects of privacy-enhancing technology on data protection and on related policy fields.

Returning for a moment to Jepperson's term, 'regime,' there are useful parallels in the recent scholarship of Sandra Braman. Braman (1989, 2004)

speaks of an emerging global information policy regime, using this term in line with regime theory in the field of international relations. She writes:

> "The dominant view of regimes is meso-level, referring to specific ways of shaping relationships among actors that embody abstract principles but are operationalised in a multitude of diverse concrete institutions, agreements, and procedures. Krasner … offered the definition of a regime that is most widely used: implicit or explicit principles, norms, rules, and decision-making procedures around which actors' expectations converge in a particular issue area … Regimes thus understood are a cooperative, sociological, mode of conflict management." (2004, p. 23-24)

This application of the regime concept bears kinship to new institutionalist thinking, relating well to Scott's pillars and carriers. In addition to the sociological connections above, we can also see in Braman's writings connections to historical institutionalism. Invoking path dependency, she stated, "it currently appears that political and economic relations of the past will be reproduced in the global information policy environment of the future" (2004, p. 11). Of unintentional consequences, she observed

> "While it may be the fancy of many that policies are always the result of intention … policy can also result from sheer chance and inadequacy in the face of complexity." (2004, p. 11)

Neo-institutionalist thought can be synthesised into three 'phases' (Lowndes and Roberts, 2013, pp. 18-45). Phase one contains scholarship from the 1930s to 1970s, encompassing the traditions and rediscovery of the 'old' institutionalism. Phase two runs from the early 1980s to the late 1990s, and sees the splitting of new institutionalism into the three major strands discussed above. Phase three begins in the early 2000s and continues on, and is characterised by convergence and consolidation. Scott (2008) is cited as a third phase institutionalist, and Lowndes and Roberts (2013, pp. 46-76) align their synthesis with his. Scott's (2008, p. 79) 'regulative,' 'normative' and 'cultural-cognitive' equate to Lowndes and Roberts' (2013, p. 46) 'rules,' 'practices' and 'narratives.'

The work of Scott, Lowndes, Lowndes and Roberts, Jepperson and Braman support the view that data protection and the protection of privacy are

institutions. Braman's conception of regime can be applied in order to analyse data protection regimes, privacy regimes, or identity management regimes. Lowndes' analytic synthesis yields an inclusive lens through which to examine empirical data. Scott's framework of pillars and carriers, building on Jepperson's work, generates clear categories by which to analyse the institutional landscape in which unlinkability policies are embedded. The scholarship detailed above allows for a comprehensive application of institutionalist thinking rather than choosing a specific camp. The regulative (rules), normative (practices) and cultural-cognitive (narratives) institutional elements of data protection and identity management are useful in explaining the policy development of unlinkability. The next section expands on the conceptualisation of data protection as an institution.

Data Protection as an Institution

Data protection is an institution. Institutionalisation is "the process whereby things become institutionalized, which, in turn, simply means that things are more or less taken for granted" (Greenwood, et al., 2008, p. 15). This is consistent with Jepperson's (1991) view of institutionalisation as the encoding of patterns in social reproductive processes. An institution is defined as follows:

> "An institution is a relatively stable collection of rules and practices, embedded in structures of *resources* that make action possible -- organizational, financial and staff capabilities, and structures of *meaning* that explain and justify behavior – roles, identities and belongings, common purposes, and causal and normative beliefs." (March and Olsen, 2004, p. 5, orig. emph.)

Data protection – and its kin, the protection of privacy – is institutionalised in liberal democracies. The state assigns resources to enact data protection: agencies, budgets, courts, lawyers, administrators, scientists and material technologies. The expectation that certain types of information will be restrained, controlled, limited, or whose transmission, storage and use are otherwise regulated is interwoven into laws, professional practices, formal and informal codes of conduct, and expectations by citizens. It has become taken for granted in many countries that the use and transmission of personal data

will be regulated in some way, though the character of that expectation is different between the two countries under study. The institution of data protection is sustained by laws, such as the US Privacy Act of 1974 or the German Federal Data Protection Directive, enforced by coercive powers to sanction. It is embedded within citizen expectations and norms of behaviour, as well as non-coercive strategies and best practices within communities. It can be seen within a 'design ethos' of computer engineers, and in the discourses of national leaders. It is a stable feature of Western political systems (Bennett, 1992), subject to change, reinvention and conflict.

Choices made by policy-makers are constrained by the institutional landscape in which information policy resides. The choices are influenced by cultural-cognitive scripts, such as the American rejection of national ID and the German rejection of an informationally intrusive state. Within the empirical research, there is evidence of a strong influence of prior policy choices informing and constraining current ones, as with the German Constitutional Court's finding of a right to informational self-determination later shaping German identity management policy. The data also can be examined from the perspective of institutional power arrangements, as with the need to include US privacy lawyers in decisions about federal identity management, though they were added in the eleventh hour, resulting in a minor struggle and a delay in the project (G010, Interview).

Scott's pillars and carriers will be used as a framework to analyse the collected data on the requirement of unlinkability. Identity management policies and the privacy and data protection choices therein are influenced by laws, administrative rules, expectations, standard operating procedures, technical protocols, system configurations (technical choices), sanctions, incentives and material technologies. By conceptualising data protection as an institution, the policy choices and forces that acted upon those elements can be analysed for the influences of other institutions, such as the market and the state, and for signs of stability or change.

Furthermore, the cases under study allow a consideration of the institutional effects of technology, protocols and standards. Unlinkability is a property of a technical system – as an analytical object, it must be considered within its material milieu. The policy choice to require unlinkability in citizen credentialing systems is influenced by the institution of data protection, and reflexively influences it. The technical components – artefacts – of unlinkability are usefully examined via Scott's regulative, normative and cultural-cognitive pillars: they are objects that comply with mandated specifications, they reflect conventions and standards, and they have symbolic value (see Figure 2.2, p. 54). The artefacts of unlinkability – cryptography, embedded chips, servers – are shaped by institutional forces, and in turn shape the behaviour of citizens. In doing so, these artefacts reproduce the institution of data protection, reinforcing and reshaping it. Katzenbach (2011, p. 125) argues:

> "… technologies can hold the status of institutions … in the sense that they embody the duality of institutions both (1) as a result of an institutionalization process: certain patterns of conduct and interpretation crystallize into material objects, technological devices or services – which then again are subject to negotiations and varieties of usages, starting another process of (de-)institutionalization; as well as (2) part of an institutional setting that facilitates, coordinates and constrains the … behavior of actors…"

Similarly, Pinch (2008, p, 466) writes:

> "Institutions have an inescapable material dimension and part of the agency that actors bring to institutions is their work in producing and reproducing (and sometimes changing) the material dimension of institutions. Likewise materiality itself exercises a form of agency and part of the agency that materiality brings to institutions is the work of producing and reproducing (and sometimes changing) the social dimensions of institutions."

The technology that enables unlinkability is a crystallisation of privacy and data protection norms and laws within both the US and Germany. Forces internal and external to the institution of data protection influenced the decisions to embed policy choices in material substrates: within the chips of the German e-ID, and within US identity management protocols and architectures. Unlinkability is an example of "institutional development" (Jepperson, 1991),

extending the earlier, core privacy and data protection goals of data minimisation, collection limitation and proportionality. Unlinkability technologies are a material result of institutional innovation, expanding and reproducing those goals. This argument conceptualises "the digital economy as an emergent, evolving, embedded, fragmented and provisional social production that is shaped as much by cultural and structural forces as by technical and economic ones" (Orlikowski and Barley, 2001, p. 154). More broadly, analysing the institutional dynamics of the technologies that underpin electronic citizen credentials helps to show how identity management policy affects and is affected by the institution of data protection.

Institutional Change

Institutionalism has been criticised for its challenges in explaining the genesis of new institutions and institutional change (Lowndes and Roberts, 2013, p. 111). By definition, institutions are recurring patterns that need little support to recur; their very reproduction, embedded in social interactions, implies stability. So, what accounts for change? Organisational theory scholars proposed an 'exogenous-shock model' where change is seen to arise from 'shocks' occurring in an institution's external environment. Later, they asserted that institutional settings were "more conflicted and pregnant with suppressed interests"; rather than stable, they were "contested terrains contoured by variation, struggles and relatively temporary truces" (Greenwood et al., 2008, p. 9). Historical institutionalism embraced its own version of the exogenous-shock model: "critical junctures," where history "branches" and institutional change occurs (Hall and Taylor, 1996). However, as Hall and Taylor (1996, p. 10) note:

> "The principal problem here, of course, is to explain what precipitates such critical junctures, and, although historical institutionalists generally stress the impact of economic crisis and military conflict, many do not have a well-developed response to this question."

In his synthetic view of institutionalisation, Scott (2008, p. 62) argues that the misalignment of the regulative, normative and cultural-cognitive pillars may

motivate different behaviours and choices, leading to confusion and conflict; conditions likely to bring about institutional change.

Lowndes and Roberts (2013, p. 143) addressed the challenges of explaining institutional change by arguing that earlier (second phase) considerations of change were preoccupied with "stop-go models driven by periodic external shocks." Instead, both stability and change are "actively constructed out of the ongoing interaction of actors, existing institutional constraints and contextual challenges," in line with the idea that institutions are contested terrains (Lowndes and Roberts, 2013, p. 130). Lowndes and Roberts reject that institutionalism is not adept at explaining change, and instead illustrate that institutionalist scholarship explains change differently according to two key variables: the tempo of change (incremental versus punctuated) and the balance between structure and agency. Mapping these together yields four perspectives on how institutions change (Lowndes and Roberts, 2013, pp. 116-132):

- Structured, incremental change: institutional change happens incrementally and as a result of structural features of institutions and their environments.

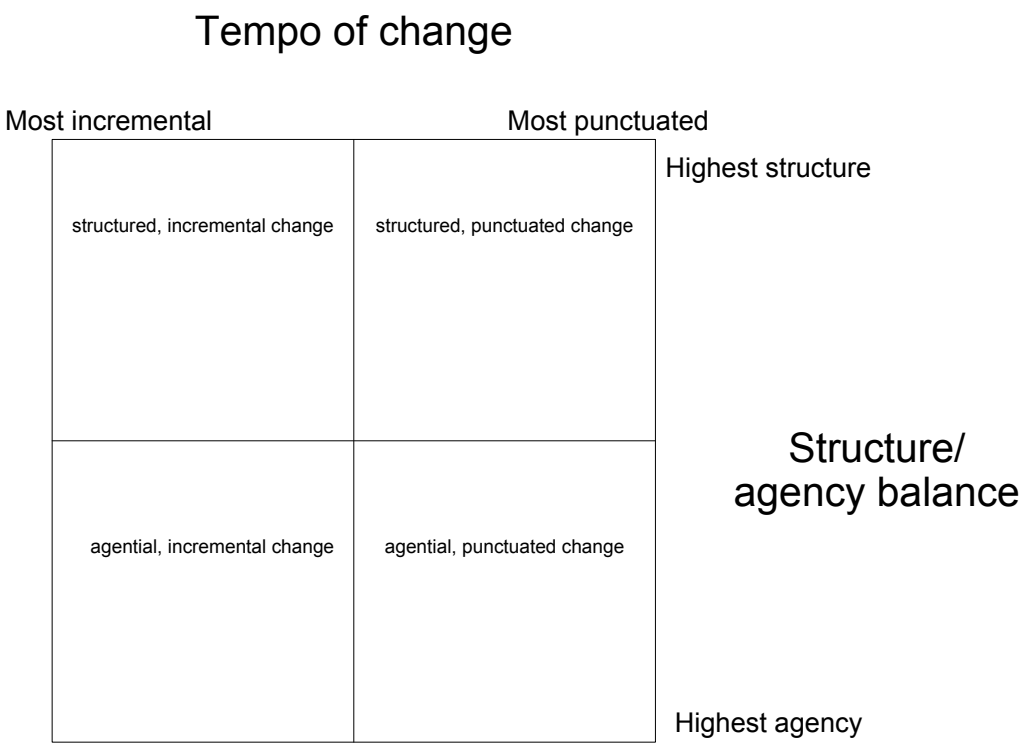
- Agential, incremental change: institutional change happens incrementally and as a result of actors making choices and imposing those choices on the world (Lim, 2010, p. 76)

- Structured, punctuated change: institutional change happens as a result of structural features of institutions and their environments, but in a punctuated way. This embraces the ideas of 'shocks' and 'critical junctures.'

- Agential, punctuated change: institutional change occurs due to the actions of agents happening in a punctuated, rather than gradual, way.

These are mapped in the figure below:

Figure 2.3 Map of institutional change explanations



Source: Lowndes and Roberts, 2013, p. 117

This study adopts this framework as a way to organise the explanations of changes within data protection that influenced the emergence of unlinkability. It facilitates comparison between Germany and the US, and further contextualises the process through which data protection is institutionalised via unlinkability. The framework focuses the contribution of the research on the tempo of the institutional development of unlinkability with respect to prior political choices. It analyses this development with regard to the balance of structural and agential factors influencing policy change.

Application of New Institutionalism to Empirical Data

To apply new institutionalism to the empirical data and enable a comparison between the two cases, Lowndes' and Scott's syntheses can be combined into a set of testable propositions related to the research questions. In the process, new institutionalism can be evaluated for fitness for use in information policy research. The propositions are:

1. *The choice to include unlinkability in citizen credentialing is influenced by formal and informal mechanisms.* A chief value of the new institutionalist approach is its exposure of the informal and the implicit. Understanding the emergence of unlinkability requires a review of all salient formal policy instruments, but an examination of the informal factors influencing policy-making is critical to a fuller explanation. This proposition addresses the calls in information policy scholarship for attendance to norms and values in policy research.
2. *There is a taken-for-granted quality to the rationale to require unlinkability.* The institution of data protection exerts influence on policy development through regulative, normative and cultural-cognitive forces. The cultural-cognitive dimension of institutions relies on them being taken for granted. The emergence of unlinkability is partly explained by this taken-for-granted quality. Attending to this sociological dimension of data protection helps to expose the values within the narratives of data protection.
3. *There is an isomorphic dimension to the choice to require unlinkability.* Isomorphism is an indication of institutional effects. The institution of data protection influences policy through coercive, normative and mimetic mechanisms. Similarities between German and US unlinkability policies may be partly explained by these mechanisms. This proposition directly addresses the comparative nature of the thesis and helps to test new institutionalism's explanatory power.
4. *Prior policy choices constrained and affected the choice to require unlinkability.* The effects of path dependence are critical to understanding the context of unlinkability policies. This proposition addresses the research question, "What is the relationship between unlinkability and historical privacy and data protection regulations?" and tests a central theory within institutionalism.
5. *Networks of social actors influence the choice to require unlinkability.* Various actors enact the institution of data protection. Their networks are pathways for institutional stability and innovation to occur. Examining the influence of these relational groups helps explain the

policy outcome of unlinkability. This proposition addresses a significant informal influence on policy.

6. *Material artefacts further institutionalise data protection.* Data protection is institutionalised through artefacts. Technology is the material dimension of this institution. The technologies of unlinkability are reflections of the institutional influences of data protection upon identity management. This proposition illustrates an implementation of unlinkability policy, and tests the institutionalist view that material technologies are carriers of institutionalisation.
7. *The requirement of unlinkability embeds the power dynamics of actors and institutional relationships*. Institutional analysis helps to show power relationships between actors and organisations, and the influences that maintain or alter those relationships. This analysis can add to the explanation of the emergence of unlinkability. This proposition addresses institutional change, highlighting the contested nature of the institution of data protection by analysing power dynamics in the policy-making process.

Taken together, the propositions capture the information policy scholars' criticisms of the field's under-theorised state: the need to analyse the norms and values influencing policy, the need to make the implicit explicit, and the call for theoretical pluralism. The propositions reflect Scott's pillars (see p. 52), encompassing a synthesis of regulative, normative and cultural-cognitive elements. The propositions focus on informal policy influences, path dependency, and material elements – critical parts of a holistic explanation of how unlinkability policies are developing. The analysis in Chapter 8 will use these propositions as a way to evaluate both the institutional effects within the German and US case data, and the suitability of new institutionalist thought to identity management research. The propositions also facilitate a direct comparison of the US's and Germany's citizen credentialing policies. The analysis will use Lowndes and Robert's (2013, pp. 117) map of institutional change discussed in the preceding section to analyse the changes within data protection that led to the emergence of unlinkability.

CHAPTER 3: METHODOLOGY

Overview

This chapter details the research design and methods of this thesis. A comparative case study was undertaken, comparing German and US identity management policies, specifically focusing on the privacy interest of unlinkability. The study was qualitative, consisting of semi-structured interviews and primary and secondary documentation review. The research design draws upon the methodologies of comparative politics and comparative policy studies. The theoretical approach of new institutionalism was applied to help explain policy development. The key purposes of the research were exploration of new phenomena and theory testing.

Research Aims

The aim of this research was to understand how privacy interests are supported by public policy as digital identity evolves in the internet. The management of digital identities and attendance to their inherent privacy challenges is a topic of much research literature in the last decade (ICPP and SNG, 2003; Hansen, Schwartz and Cooper, 2008; OECD, 2007, 2009; Lips, Taylor and Organ, 2009a, 2009b; Lusoli, Maghiros and Bacigolupo, 2008; van der Hof, Leenes and Fennell, 2009; Pfitzmann and Borcea-Pfitzmann, 2010; European Network and Information Security Agency, 2011; FIDIS, n.d; PrimeLife, n.d.). Scholars and practitioners have drawn attention to the importance of designing systems that enhance the privacy of users and give them greater degrees of control over the storage, use and sharing of information about their online lives (Bhargav-Spantzel, Camenisch, Gross and Sommer, 2007; Hansen, 2008b; Leenes, 2008). In particular, there is recognition that 'linkability' – the linking of data

and activity to a specific person, yielding a detailed, sensitive profile – is a salient and important topic in the field of identity management (Hansen, 2008a; Landau, Le Van Gong and Wilton, 2009; Storf, et al., 2009). This research addresses this topic by providing empirical data and analysis of two countries' attempts to employ 'unlinkability,' the severing of links so as to separate contexts and frustrate profiling, in their citizen credentialing initiatives. The thesis applies the new institutionalist theoretical approach to explain the policy development of unlinkability in the two countries, and to test its efficacy for use in identity management and privacy policy research.

The research questions are:

- How is unlinkability emerging as public policy?
- What is the relationship between unlinkability and historical privacy and data protection regulations?
- What are the similarities and differences between US and German unlinkability policies?
- To what extent can new institutionalism explain the emergence of unlinkability?

By answering these questions, this research adds empirical data and analysis to the fields of identity management, privacy and information policy, and illustrates the connection between historical privacy and data protection interests and current policy dilemmas. It contributes to an understanding of citizen credentialing and the policy instruments being employed to protect citizens' privacy with regard to digital identity. By comparing the US and Germany, a greater understanding of each country's identity management initiatives can be achieved than what could be understood by studying each in isolation.

Research Methods

The central method of this research is the comparative method, drawn from the field of comparative politics. This field "examines the interplay of domestic and external forces on the politics of a given country, state, or society" (Lim, 2010, p. 13). Comparison is the "principal method" to test theory in political science (Peters, 1998, p. 1). Within comparative politics, this research falls into the category called comparative policy analysis, or comparative public policy. Heidenheimer, Heclo and Adams (1990, p. 3) define comparative public policy as "the study of how, why, and to what effect different governments pursue particular courses of action or inaction." They further state:

> "… comparative policy analysis occupies a middle ground between 'pure research' of a theoretical nature and 'applied science' directed towards the nuts and bolts of detailed problem-solving…. It also helps us test general theories and hypotheses by exposing the varied nature of political decision making as it confronts concrete issues."
> (Heidenheimer, et al., 1990, p. 2)

This research methodology has been used comprehensively in prior policy research on privacy issues by Bennett (1992) in *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*. In this work, Bennett argued that policy problems related to informational privacy and data protection were "clearly … amenable to analysis using the theoretical and methodological tools of the political scientist" (1992, p. 2). In the present research, the 'how' and 'why' of particular information policies are the primary foci. As 'to what effect' the pursuit of unlinkability yields, this research analyses the technical implementation of policies, but given the youth and immaturity of the policies, an assessment of their impact on citizens or their efficacy in relation to original policy goals would be premature.

This research also relies upon literature review. The study was interdisciplinary and used a wide range of primary and secondary literature: laws, policy documents, administrative memoranda, posts on official blogs, commercial

white papers, trade association position papers, government requests for proposals, official technical guidelines, legal analysis, international standards, technical architecture documents, lexicons, government reports and testimony, and academic journal papers and book chapters. Literature selection was thematic and purposive – strategically chosen for relevance to the research questions – and the selection 'snowballed'; documents in one area would lead to additional papers and sources (Bryman, 2012, pp. 418-424). The literature review is comprised of several academic disciplines: political science, law, sociology, computer science, and policy studies.

To facilitate comparison and fully explicate the policies of unlinkability and citizen credentialing, this thesis follows McClure, Moen and Bertot's (1999) methods for descriptive assessment of information policy initiatives. These methods help to provide "a gestalt or multidimensional view of an information policy initiative" (McClure et al., 1999, p. 314). The empirical data chapters present a holistic picture of the emergence of unlinkability policies, examining formal policies, their origins and proximate influences, legislative and judicial relationships, individual and organisational actors, and political and commercial influences. This formal examination is then augmented with the application of institutional theory so as to analyse the informal, tacit, relational and cultural dimensions of policy formation.

The research employs a comparative case study strategy, which is appropriate to investigate the emergence of unlinkability. Benbasat, Goldstein and Mead (2002, p. 96) state, "case strategy is particularly well-suited to [information systems] research because the technology is relatively new and interest has shifted to organizational rather than technical issues." Yin (2009, p. 18) states that case study is used when the "boundaries between phenomenon and context are not clearly evident." The limited degree of empirical research into the policy development of unlinkability, the intersection of organisational and

technical subjects, and the prevalence of case-based research in policy and political science support these rationales. The case study type is 'intrinsic' – the particulars of the cases themselves are important, versus using the case to examine or demonstrate another topic (Stake, 1995, p. 3). The intent of the study is particularisation rather than generalising. Case study is also well-suited to theory testing (Yin, 2009, p. 36). As such, this research tests the new institutionalist theoretical approach against the empirical data on identity management and unlinkability.

To explain the similarities and differences in the development of unlinkability policies in Germany and the US, the research follows the 'most similar systems' design (Meckstroth, 1975; Peters, 1998, pp. 37-41). In this design, the systems being compared are largely similar along a range of political and social phenomena in order to 'control' for those factors, and then seek out other factors that led to the development of a particular policy. Two cases were chosen to examine how unlinkability was emerging in public policy, Germany and the US. The comparison of two or a similarly low number of cases is known as 'small *N*' research (Peters, 1988, pp. 68-69). The small number of cases has inherent challenges. By examining two countries which, while similar, still have very diverse histories and cultures, it becomes difficult to isolate explanations that neatly apply across both. Anckar (2008, pp. 389-390; see also Peters, 1998, pp. 65-69) writes:

> "Although theoretically robust, the [most similar systems design] suffers from one serious practical shortcoming. There are a limited number of countries and therefore it will never be possible to keep constant all potential explanatory factors."

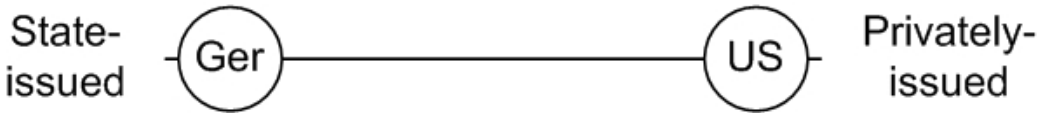
The two ways to address this shortcoming are to focus on "a single institution, policy or process" (Peters, 1998, p. 67) and restrict "the analysis to the key variables and omitting those of only marginal importance" (Lijphart, 1975, p. 159). In the present research, the focus is on the policies of unlinkability. These

policies can only be understood in the context of identity management policy, e-government initiatives, and data protection and privacy policy. Further, single case studies and comparative studies of two countries are established methods of analysing political phenomena with the new institutionalist approach (Steinmo, Thelen and Longstreth, 1992). The goal of particularisation and the aim of understanding the institutionalisation processes leading to unlinkability in Germany and the US necessitate a great deal of empirical depth, which in turn limits the number of cases due to time and resources.

Case selection was based on a number of factors. First was the 'most similar design' model: Germany and the US are both liberal democracies with federal governments, are technologically advanced nations with mature economies, and have federal-level data protection regimes. Both were in the midst of developing or implementing citizen-focused digital identity management policies in the same timeframe, and both included unlinkability in their technical designs. The policies in question were being developed at the federal level in both countries without variation or influence by state-level policies. There were important differences that would enable a rich comparison. Germany has an omnibus data protection law covering all instances of 'personal data,' whereas US data protection is sectoral. Germany has a data protection policy 'layer' in the form of a federal data protection commissioner and state data protection authorities; the US lacks an equivalent. In Germany, citizen credentials were being issued by the state. The online credentials where unlinkability was to be found were derived of Germany's electronic national ID card, issued in 2010. The 'identity supply chain' was completely under the control of the German Ministry of Interior. The Ministry coordinated the enrolment of citizens and residents via local municipal offices, managed and paid for the cards to be created with identity data loaded onto them, and returned them to the municipal offices for distribution. This made the identity an official one, derived from data held and validated by the state. The German

processes and policies are fully detailed in Chapter 6. The US, in contrast, has no national ID card and, as Chapter 5 explains, it was politically impossible to deploy one, even one restricted exclusively to e-government. Consequently, the US elected to rely upon privately-issued credentials from companies like Google and Yahoo!, and from universities and research institutions. If one conceives of a spectrum of state-issued to privately-issued credentials, Germany and the US fall on either side:

Figure 3.1 Spectrum of credential issuance sources



Using these two issuance categories as a criterion for case selection is a form of 'generic purpose sampling' (Bryman, 2012, p. 422). In this sampling strategy, *a priori* and fixed categories that are relevant to the research questions are used as criteria for selection. At the outset of the research, it was assumed that these two categories – state vs. private issuance – were the primary issuance methods of citizen credentials.

The similarities and differences above support the rationale of selecting Germany and the US. The other key factor in choosing these cases was their accessibility. Through an internship and subsequent employment with Experian, a credit reference and marketing information company, a valuable set of contacts who could introduce stakeholders in both Germany and the US became available. With American citizenship, entry and travel within the US was unproblematic. A wide network of friends and offers of accommodation would assist in keeping costs down. Traveling in Germany was also easy as no visa was required.

The thesis is a work of qualitative research. The policy phenomena under study is recent, in limited degrees of implementation, and involves the contributions of a plurality of stakeholders who held a variety of views. Quantitative research tends to focus on the numerical quantification of phenomena in a structured way (Bryman, 2012, p. 408). It aims at generalisation, and the relationship between the researcher and participants can be seen as 'distant' (Bryman, 2012, p. 408). Qualitative research is more concerned with contextual understanding of rich data (Esterberg, 2002, p. 2). The researcher is 'close' to her or his participants, and it is better suited to particularisation (Bryman, 2012, p. 408). However, there is debate over the ostensible contrasts between qualitative and quantitative methods (Hammersley, 1992). While some scholars note that qualitative research is less concerned with theory testing (Esterberg, 2002, p. 7), others view qualitative methods as well-suited to it (Bryman, 2012, p. 387; Silverman, 2001, p. 71). To understand the policy's development, it was important to explore values, norms, goals, intentions, technical designs and history. Bryman (1988, p. 65) observed: "… whatever the sphere in which data are being collected, we can understand events only when they are situated in the wider social and historical context." To comprehensively tell the 'story' of unlinkability, a qualitative research design was called for. This would allow 'thick description' (Geertz, 1973) of a largely unexplored empirical domain. The limitation of particularisation is that the research does not lend itself to generalist explanations of phenomena.

To understand the development of unlinkability, it must be placed within a social, historical and cultural context. Those contexts are particular to each country under study, supporting a particularist approach to the research design. The particularist nature of this thesis is consistent with the analytic goals of new institutionalism, which also seeks to place policy choices within a social, historical and cultural context. The limitation of this approach is the difficulty in drawing general analytic conclusions from the research.

Qualitative research is concerned with process (Bryman, 1988, p. 65). This comports well with studies of new policy phenomena. Unlinkability and privacy studies generally must account for norms and values as much as they account for prior policy, economics, history and technical issues. "The most fundamental characteristic of qualitative research," Bryman argued, "is its commitment to viewing events, action, norms, values, etc. from the perspective of the people who are being studied" (1988, p. 61). Semi-structured interview is a valuable method to accomplish this. It allows access to subjects' accounts of the values and norms underpinning the policy development of unlinkability, and details of informal policy influences, such as cultural phenomena and professional relationships. Semi-structured interview is thereby a strategy to enable value-critical analysis of information policy subjects. It supports McClure and Jaeger's (2008, p. 258) call for information policy research to explain "conflicts between policies and stakeholders, [excoriate] assumptions and values, [and offer] guidance in articulating conflicting issues.…" In line with new institutionalism, semi-structured interview facilitates the analysis of how actors' choices are influenced by norms, cultural beliefs, narratives and past decisions.

Qualitative methods have been used in prior information policy research. Van der Hof, Leenes and Fennell (2009) undertook eight case studies on the changing nature of identity construction and citizen-government relations in relation to uses of identity management and information technology by the Dutch government using document analysis and semi-structured interview as chief methods. Lips, Taylor and Organ (2009b) used similar qualitative techniques in eight case studies of new uses of identity management technologies in UK public services to explore changing informational relations between citizens and the state. Noack and Kubicek (2010) used qualitative interviews to research the origins of the online authentication features of the

German e-ID. Kim, Kim and Lee (2009) used a single case study and semi-structured interviews to examine a Korean anti-corruption e-government system. Weerakody, El-Haddadeh and Al-Shafi (2011) used case study and interview to understand the diffusion of e-government in Qatar. Burt and Taylor (2007) used qualitative methods to gain a holistic understanding of the use and impact of Scottish Freedom of Information requests. Bennett (1992) used primary and secondary document analysis and elite interviewing in his comparative study of the data protection policies of Sweden, the US, West Germany and Britain. He sought to build 'contextual and experiential knowledge' (1992, p. 10, citing Anderson) of his subject, observing:

> "It is more messy, more inductive, less definitive, but probably more faithful to political reality." (Bennett, 1992, p. 10)

This thesis joins these other publications in the use of qualitative methods to holistically examine information policy phenomena.

Data Collection

Primary and secondary documentation was reviewed to understand the issues and technologies of privacy and data protection within identity management, and to incorporate prior relevant research. Document selection was purposive and it snowballed, as described above. Literature sources were derived from coursework, academic journals, books, blogs, and websites. Academic publication databases, such as ProQuest, JSTOR, and Science Direct were searched with combinations of keywords, including "identity management," "IDM," "privacy," "data protection," "PETs," "institution," "institutionalism," "institutionalist," and "information policy." A set of academic publishers contained a disproportionate amount of relevant literature, so further searches were focused on them: Springer, Elsevier, and Taylor & Francis. Certain authors recurred throughout the research, so their publications and references were specifically targeted (see Bibliography for complete citations):

M. Hansen, W. Scott, V. Lowndes, G. Hornung, R. Leenes, J. March & J. Olsen, P. DiMaggio & W. Powell, J. Taylor, R. Clarke, C. Bennett, S. Braman, A. Pfitzmann and M. Lips.

To gather respondent data, semi-structured interviews were carried out with a wide variety of stakeholders. The sample of respondents was purposive and augmented by snowballing, where initial respondents identified other suitable subjects (Bryman, 2012, p. 424). A list of interview subjects and/or their roles is included in Appendix A. Respondents were selected for their connection to or influence over the policy-making process, because they had done research on related topics, or for their role in policy implementation. The sample contained policy elites, bureaucrats and administrators, government lawyers, privacy advocates, data protection authorities, businesspeople, academics and researchers. Twenty-eight interviews were conducted for the US case, three of which were in a group interview. For the German case, fourteen interviews were conducted; one in a group of two, and one in a group of four. All interviews were conducted in English. One German interview required the presence of a translator. He was not a formal, trained translator; he worked in the same organisation in a related field and was asked by the subject to be present. The main subject spoke English through the majority of the interview, but gave German answers to the translator for a small number of questions where his command of English failed him. One US interview subject declined to be interviewed and one did not respond to multiple requests. This was mirrored in the German case – one refusal and one failure to respond. On the whole, access problems were minimal and nearly everyone needed to provide a holistic picture of unlinkability policy development were interviewed.

There were fewer German interviews because German citizen credentialing policy was more mature than that of the US. In late 2010, German e-IDs replaced their prior paper IDs – by this point, the development of identity

management and unlinkability policies was effectively complete and in a stage of advanced implementation. The US in contrast was still in a state of flux. During the field research period, initial implementation was still iterative, new significant policies were being developed, and initial identity management policy goals were not close to being achieved. Further, national identity policy, a precursor to citizen credentialing, was well developed and institutionalised in Germany; not so in the US. To best understand the policy inputs and outputs, the various influences, and the likely policy direction, a wider group of US stakeholders had to be interviewed.

A topic guide was created for the interviews. It focused on the origins, genesis and justification of unlinkability policies, the broader policy landscape of identity management and citizen credentialing, stakeholder identification, institutional influences, the state of policy implementation and the challenges therein. The topic guide was separated into Policy and Technical sections to accommodate the variety of interview subject roles. The questions and topics came from an understanding of general public policy processes from prior coursework, e-ID and identity management literature, institutionalist literature, comparative policy literature, an understanding of IDM business issues from time spent working at Experian, an understanding of technical projects from previous work as a technologist, and suggestions from supervisors. The topic guide was influenced by Bennett (1992, p. 11), whose interview questions "were directed toward gaining an appreciation of the specific reasons that brought the issue to the agenda, of the most important actors in the policy-making process, and of the wider impact of international and domestic factors on the countries in question." See Appendix B for the topic guide used in the interviews.

All of the interviews, American and German, were rich and detailed, running an average of ninety minutes each. The audio of the interviews was recorded

onto SD card with a digital recorder, and notes were taken throughout. The topic guide was followed and adapted to subjects' specific roles, though subjects were also allowed to roam to related issues if they were germane to the overall research questions and context.

US Interviews took place in seven cities: Washington D.C.; Mountain View, CA; Seattle, WA; Boston, MA; Gaithersburg, MD; Bethesda, MD; and, Silver Spring, MD. German interviews took place in Berlin, Bonn, Bremen, Darmstadt, Kiel, Kassel and Köln. Interviews took place in many settings – hotel lobbies, civic centres, the Google campus, the MIT campus, over Skype and the phone, in government buildings, and inside a Krispy Kreme donut shop on a lonely stretch of road in Seattle, Christmas music playing in the background.

Interviews were transcribed by a confidential commercial service. A list of key terms, acronyms, proper names and foreign words was supplied to the service to aid transcription. The service was instructed to delete each audio file and all transcript data once the transcript was approved. Transcripts were reviewed against the original audio files for correctness. Backups of the recordings were stored on Dropbox, an encrypted cloud-based file storage service, also only with identifiers (Dropbox, n.d). There were additional backups burned to DVD that were always in my physical possession. All data was removed from Dropbox at the conclusion of the research.

For subjects who elected anonymity, identifying information was removed from the filenames and metadata of the audio files. US subject identifiers began with 'G' for government stakeholders, 'N' for non-profit staff, and 'P' for for-profit staff. Interviews were numbered sequentially excepting those who declined anonymity. For example, the third government stakeholder interview was denoted as 'G-003,' while Dazza Greenwood's interview was

denoted, ‘DGreenwood.’ German interview identifiers were prepended with ‘DE’ except for those waiving anonymity. A spreadsheet was maintained containing a list of all possible and desired interview subjects, including their organisation, role and focus area, why they should be interviewed, how they came to be selected (via literature or another person), where they were based, when the interview occurred, and whether they elected anonymity or not. This was done for both US and German subjects.

Analysis

Once all interviews were transcribed, they were coded using thematic analysis based on the research aims, questions and findings (Braun and Clarke, 2006). Thematic analysis is “essentially independent of theory and epistemology, and can be applied across a range of theoretical and epistemological approaches” (Braun and Clarke, 2006, p. 79). Thematic analysis locates patterned responses and meaning across a corpus of data. The themes identified were both inductively derived from a close reading of the data in union with an understanding of the problem space from literature and professional experience, and driven by an institutionalist theoretical approach. The themes were identified at a ‘semantic’ level:

> “With a semantic approach, the themes are identified within the explicit or surface meanings of the data and the analyst is not looking for anything *beyond* what a participant has said or what has been written. Ideally, the analytic process involves a progression from *description*, where the data have simply been organised to show patterns in semantic content, and summarised, to *interpretation*, where there is an attempt to theorise the significance of the patterns and their broader meanings and implications … often in relation to previous literature.” (Braun and Clarke, 2006, p. 89)

Thematic analysis is not a linear process. During interviews, when reviewing notes, while correcting transcripts and throughout document reviews, items of interest and potential themes were noted and revised. Once transcripts were

ready for coding, those items and themes were organised into a set of eight category headings: Fraud and Risk, Business, Policy, Architecture and Standards, Culture, Players, Faces of Identity, and Usability. Under each category was a set of codes to help organise the data into manageable groups. A colour was assigned to each category heading and the first interview was coded. The categories maintained their utility throughout the interview, but there were a number of emergent codes not captured in the codebook, so the process was reiterated twice more. The codes, themes and categories ultimately stabilised and were applied across the entire set of interview data. From this, a set of themes emerged that connected both cases, and ones that were particular to one or the other case.

All of the research subjects' views are represented in the thesis, including minority views. The following table lists the frequency of the appearance of respondents within their respective data chapters, the policy comparison chapter (Chapter 7), and the application of theory chapter (Chapter 8).

Table 3.1 Frequency of respondent references

US	Total
G001	34
G003	30
G004	11
G006	13
G007	12
G008	5
G009	5
G010	5
N002	8
N003	21
N004	6

Germany	Total
DE-G001	17
DE-G002	23
DE-G003	17
DE-G005	7
ULD	36
JFromm	37
Hornung	19
Kubicek	22
Möller	34
Margraf	3

N005	12
N006	9
DonT	11
DReed	6
SDavid	6
RWilsher	13
BMorgan	22
DGreenwood	7
P001	16
P005	2
P006	10
P007	2
PaulT	7
Nash	6

The empirical data chapter on Germany is 20% shorter than the empirical chapter on the US. This is because German policy is more mature, more coherent, and fewer stakeholders were involved with policy development. As those chapters and Chapter 6 explains, German e-ID activities grew out of its prior national ID and e-government initiatives; the path from these policy inputs to the e-ID was 'straighter' than the US path to its IDM initiatives. The US had no prior national identification policy infrastructure, and its data protection influences were also less coherent than Germany's. Prior pseudonymity requirements in other laws and the influence of Germany's data protection authorities contributed to a more direct narrative of policy development. The larger number of key actors and commentators in the US – largely resultant of US reliance on the private sector and intermediaries – and the more formative state of its identity management policies necessitated a greater number of interviews and lengthier policy narrative.

The referencing in this thesis follows the Harvard APA system. Within the text, where the author's name is long, the full name is given in the first instance

of the reference followed by brackets that contain an abbreviation that will be used in all subsequent in-line citations. In the case of an interview subject, the first appearance of the reference contains the subject's full name followed by brackets containing only the last name, which will then be used in all subsequent in-line citations. As per Harvard APA guidelines, interview subjects are not referenced in the bibliography.

Ethics

All interview subjects were presented with a Consent and Information form prior to data gathering. The form detailed the nature of the research, how a subject's data would be used, a pledge of confidentiality and anonymity, and contact information for the manager of the Doctoral Training Centre for any questions or issues. Subjects were given the opportunity to waive anonymity before or after being interviewed, and to withdraw from the study at any point. Signing the form was deemed to be an act of informed consent. The form and research design were submitted to a school ethics committee for review prior to embarking on field research.

Summary

This chapter detailed the research aims, questions, design and methods used in this thesis. The aim of this research is to understand how public policy can support privacy goals with regard to the growth of digital identity. To accomplish this, a comparative case study design is used. The research explores the emergence of unlinkability in the identity management policies of Germany and the United States. There are key similarities between the two countries – they are both federal systems, economically advanced, and liberal democracies. Both countries also have privacy and data protection frameworks at the federal level, and both have embarked on e-government and identity management initiatives for citizens in the last decade. There are key

differences as well: the US is nearly four times the population of Germany, and Germany is part of the supranational European Union whereas the US is an independent nation. Germany has an omnibus data protection framework plus federal and state-level data protection authorities. The US has a sectoral data protection framework and no data protection authorities. Both countries have policies requiring or encouraging unlinkability within their citizen credentialing initiatives.

The thesis falls within the category of comparative policy studies, though it draws upon sociology, organisational theory, law, political science, and computer science scholarship. Chapter 2 explains that the research's primary discipline is information policy, a multidisciplinary field. It discusses the need for attendance to the institutional dimensions of information policy, and informal policy influences such as values, norms and relationships. The thesis answers this call by applying the new institutionalist theoretical approach to the case data, also explained in Chapter 2. The thesis uses a qualitative research strategy due to the need to explore values, norms, history, narratives and technical artefacts. The policy under study is new and in the US, still evolving – this and the institutionalist approach of placing policy in its historical, social and cultural context supports a qualitative research strategy. The main methods employed were semi-structured interview, which provides access to accounts about values, norms, goals and cultural beliefs, and primary and secondary document analysis. Thematic content analysis was used to code and analyse the data. A total of forty-two interviews were conducted in fourteen cities in two countries. Policy-makers, administrators, data protection officers, engineers, consultants, advocates, government lawyers, academics, trade groups and members of industry were among the stakeholders interviewed.

The German case lacked a privacy advocate respondent, which would have added further diversity to that case's stakeholders. Other respondents discussed

the role of one key advocate, who did not respond to requests for an interview, during the development of German e-ID policy. Further, a similar role – one highly sceptical and critical of government plans – was played by the ULD, a key German data protection authority. Still, the voice of the Chaos Computer Club, a group opposed to the e-ID in general, would have been a useful addition. In the US case, no academic voices were included, due to the near total absence of American scholarship on national identity management issues. In both cases, citizens' voices were not represented. While the thesis is focused on policy development, less so on policy outcomes, there were issues discovered during analysis that implicated citizens; usability, in particular. Further time and resources would have been needed to gather data from citizens in both countries.

Upon reflection, the method was fit for purpose. It successfully elucidated the informal policy influences on unlinkability as well as the formal. The use of semi-structured interview drew out data that was amenable to institutionalist analysis. The qualitative research design allowed for unlinkability policies in Germany and the US to be placed into a historical, social and cultural context, enabling a rich understanding of policy development.

CHAPTER 4: KEY TERMS AND CONCEPTS

Introduction

This chapter provides information on the key terms and concepts of this thesis. In line with the research questions and empirical data, the main topics are unlinkability, identity management and citizen credentialing. To understand the policies under study, it is first useful to clarify the technologies that underpin them. Information policy is often a highly technical domain, which has the potential to render the field opaque to non-technical researchers. Standards, protocols and technical architectures are themselves policy instruments. This is true for the present research, and it supports the view that information policy is a multidiscipline. As with most technical subjects, the 'devil' is in the details. This chapter presents the most important terms and concepts for a holistic consideration of unlinkability so that students of information policy may understand the nuances without prior extensive exposure to complicated technical subjects.

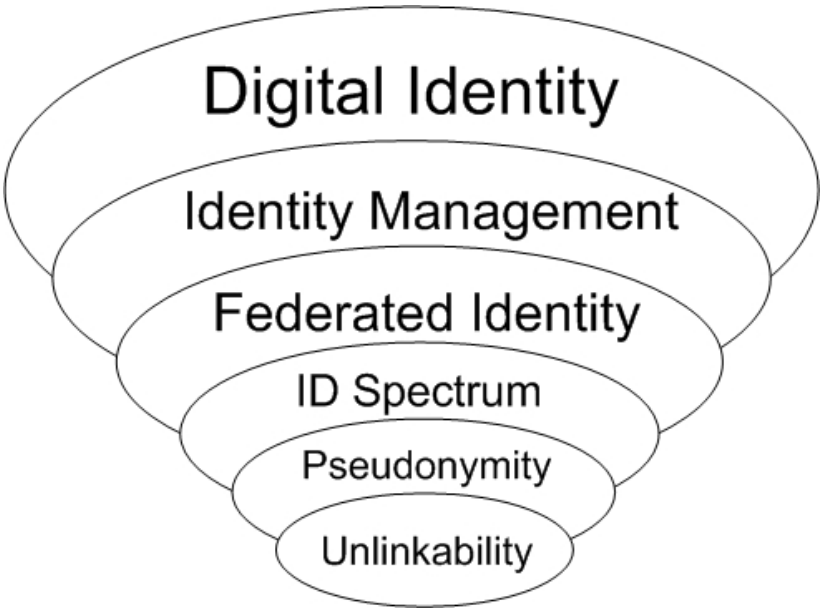
Unlinkability is both a strategy and a characteristic of a technical system, and the term overlaps with a number of other related terms, such as pseudonymity. To complicate matters, the term unlinkability does not appear in many of the salient policy instruments of the US and Germany. Moreover, the term tends to appear in European documents rather than American; infrequent appearances in US policy documents often make reference to a specific European taxonomy (McCallister, Grace, and Scarfone, 2010; Pfitzmann and Hansen, 2010). This thesis contributes to information policy scholarship by uniting US and European terminology across a range of policies, technologies and strategies.

Unlinkability is a technical characteristic of a digital identity management system. The first section progresses towards an explanation of unlinkability by

discussing ‘digital identity,’ synthesising a number of proposed definitions. The next part explores how these identities are managed in dedicated systems, followed by an examination of one specific management architecture known as ‘federated identity.’ Both the German and US cases rely on federated identity systems, one based on e-ID cards, the other on ‘soft’ credentials. Federated identity means signing in once and being able to access multiple unrelated resources.

To lay the groundwork for later discussions of privacy and data protection, the ‘ID spectrum’ of anonymity to full identification is explained. This part discusses pseudonymity, a critical element of unlinkability. The section concludes with an explanation of the technical characteristics of unlinkability, and situates it within privacy and data protection imperatives. Taken together, the above topics sketch out the necessary technical backdrop to understand

Figure 4.1 Nested topics to understand unlinkability



unlinkability sufficiently to analyse it as a policy choice. Figure 4.1 above shows how the topics nest within one another.

The second section explains the nature of citizen online credentials within the context of e-government. For over a decade, governments around the world have been building identity systems to enable their citizens to login to public and private websites with trustworthy credentials. Both US and German citizen identity management efforts have advanced in relation to a growth in e-government activity. The two empirical chapters explore this relationship in depth. This section explores the difference between 'hard' and 'soft' credentials, and discusses state issuance of them versus private issuance. Germany is a case of state-issued hard credentials in the form of an e-ID card. The US is a case of privately-issued soft credentials, existing only online. Key definitions and technologies are described, as well as inherent privacy and security challenges. Fundamental citizen identification issues are discussed and related to the main topics.

Unlinkability

This section explains the nature of unlinkability by laying out the conceptual and technical frameworks in which it occurs. Various definitions of digital identity, identity management, federated identity and pseudonymity are synthesised. Unlinkability is then defined and related to the protection of privacy.

What is digital identity?

The root of the considerations of this research is a human being, which can be called an 'entity.' Clarke (2010, p. 4) defines an entity as such:

> "An entity is a real-world thing. The notion encompasses pallets piled with cartons, the cartons, and each item that they contain; plus artefacts such as computers and mobile phones; and animals and human beings."

Non-human entities are beyond the scope of this research. Ergo, all entities discussed herein are unique, living people. An entity has multiple 'identities.' While identity is a fluid concept, consisting of self- and socially-constructed aspects, here it is understood to be an external perspective, what Hildebrandt, Koops and de Vries (2008, p. 8) call "*idem*-identity":

> "*Idem*-identity is the third-person attribution of sameness: 'This is Miss Cheung, a blond female executive'; it takes an objectified perspective."

Idem-identity and its counterpart, *ipse*-identity, or selfhood, are based on the work of the French Philosopher, Paul Ricoeur (Hildebrandt, Koops and de Vries, 2008; van der Hof, Leenes and Fennell, 2009; OECD, 2007). *Idem*-identity is the focus of this research because the policies being examined relate to external organisations – the state and private ones – assigning identities to people. This external notion of identity also allows one to construe identity as a collection of 'attributes,' or characteristics. Accordingly, Pfitzmann and Hansen (2010, p. 30) define identity as:

> "… any subset of attributes of an individual person which sufficiently identifies this individual person within any set of persons. So usually there is no such thing as 'the identity', but several of them."

These multiple identities can be termed 'partial identities,' as none of them could ever comprise the totality of the entity which they describe and refer to (Bauer, Meints and Hansen, 2005, pp. 52-53). A partial identity therefore individuates a person in a particular context via a set of attributes. Clarke (2010, p. 4) expands on the contextual nature of partial identities:

> "A person (whether a human, or a legal entity) may … present many identities, to different people and organisations, and in different contexts. Each identity can be thought of as a presentation or role of an underlying entity. Examples important in eCommerce and eGovernment include customer/client, supplier, employee and contractor."

Similarly, Pfitzmann and Hansen (2010, p. 31) affiliate partial identities with contexts and roles:

> "An identity of an individual person may comprise many partial identities of which each represents the person in a specific context or role. A partial identity is a subset of attribute values of a complete identity, where a *complete identity* is the union of all attribute values of all identities of this person. On a technical level, these attribute values are data."

This partial identity requires an 'identifier' to individuate the underlying entity in a given role. An identifier is "one or more data-items concerning an identity that are sufficient to distinguish it from other instances of its particular class, and that is used to signify that identity" (Clarke, 2010). The international standard, ISO/IEC 24760-1 (2011, p. 10), defines an identifier as:

> "… [a] reference to a unique object that is used by an entity to be uniquely represented within a specific domain or process; the purpose of an identifier is to provide entities with means of representation independent of the entity's identity in a given context without necessarily revealing the entity's identity…."

In union, these terms establish that an identifier represents an entity, individuating her or his partial identity from other humans in a given context. An identifier is a piece of data that may or may not reveal the underlying 'true' identity, here understood to mean the set of information that can disaggregate a human from all other humans.

Clarke's definition of an identifier as a 'data-item' and Pfitzmann and Hansen's statement that attribute values are data drive these terms closer to a conception of digital identity. Complementing the data-centric view of identity is Thierry Nabeth's (2009, p. 36, orig. emph.) distinction that identity can be approached from a *structural* perspective and a *process* perspective:

> "**1. A structural perspective: Identity as a representation.** *Identity* is seen as a set of attributes characterising the person.

> **2. A process perspective: Identity for identification.** *Identity* is considered according to a set of processes relating to disclosure of information about the person and usage of this information."

The empirical research of this thesis encompasses both of these perspectives, and so must a definition of digital identity. The structural perspective is descriptive, and from a data-centric view is understood to be records of a person's characteristics and the identifiers that refer to him. The process perspective implies the use of those records to achieve some aim. This distinction helpfully separates 'identity' from 'identification.'

Borrowing the term 'persona' from Jungian psychology, Clarke (1994a) defined a 'digital persona' as "a model of an individual's public personality based on data and maintained by transactions, and intended for use as a proxy for the individual." This idea comports with both the structural and process perspectives of identity, and implies an association with an identifier. Broader but related is Cameron's (2005) definition of a 'digital subject': "a person or thing represented or existing in the digital realm which is being described or dealt with." Clarke (1994a) distinguishes between "informal digital personae based on human perceptions, and formal digital personae constructed on the basis of accumulations of structured data." The formal digital persona is a data-centric conception of *idem*-identity. Building upon this, Clarke (1993) defines digital identity:

> "Digital identity is the means whereby data is associated with a digital persona."

In line with Clarke, Cameron, Nabeth, and Pfitzmann and Hansen, another useful definition of digital identity is:

> "Digital identity should denote all those personally related data that can be stored and automatically interlinked by a computer-based application." (ICPP and SNG, 2003, p. 6)

While this definition lacks Clarke's 'transactional' component of a digital persona, it retains the structural and process perspectives of identity (storing and interlinking). Clarke's conception of the transactional nature of digital identity is vital, though. An entity is a living person – the structural components of the person's digital identity are descriptors, identifiers, and attributes stored in a computer. The processes related to the person's digital identity must invariably invoke some of this stored data. Those invocations are transactions, also known as 'claims.' Claims can be made by a subject entity ("I am Gilad Rosner, and my account number is 123456"), or on behalf of a subject entity ("Gilad Rosner's credit score is 800"). As such, one author of an OECD (2007, p. 40) report on "Digital Personhood" defines digital identity as:

> "… the combination of two elements: an identifier and a collection of claims.… An identifier is simply a name – it can be a name which is comprehensible to a human … or a name which is comprehensible to a computer system.… A digital identity's identifier refers to the identity's collection of claims."

Here, information about a person – height, eye color, name, bank account number, education level attained – is equalised to the level of a claim, corroborated or uncorroborated. Similar to the OECD report is Cameron's (2005) definition of digital identity in his "Laws of Identity" paper: "a set of claims made by one digital subject about itself or another digital subject." The claims-based model captures a transactional conception of identity, but discards notions of selfhood, personal data and the distinction between an entity and its attributes.

The terms and concepts discussed are contentious and overlapping. Considerations of digital identity are context-bound, and the above examination is meant to place boundaries – albeit fuzzy ones – around a fluid set of ideas to provide enough information to understand unlinkability and its emergence as public policy. For the remainder of the thesis, the definition of digital identity is as follows: *Digital identity is a set of information and*

attributes that can disaggregate a person from all other persons within a given context. It is transactional and composed of data, and is represented by an identifier which may or may not reveal the full identity of the underlying person.

This definition synthesises the ones above in a way that is most useful to the empirical research. Further, the digital identities discussed herein are understood to be *organisationally governed*, meaning that the records and transactions comprising the identities are 'owned,' held, managed or originated by public and private organisations. In the US case, corporations and universities 'own' the identities – the data lives on their servers, and its disposition is under their control. In the German case, they originate with the state and are held on an e-ID card. The empirical data chapters 5 and 6 explain the organisational governance in detail. The next section explores how digital identities are managed.

What is identity management?

For digital identities to function they must exist within a technical framework – they must be managed. In this sense, they are not unlike products. Nabeth's (2009) structure/process perspectives are again useful: digital identities are structured pieces of data, claims are sets of procedures, and management of the whole enterprise is a process accomplished through a structural system made up of infrastructure and human and non-human actors. A paper produced by HP Labs defines identity management:

> "The term 'identity management' is currently associated to technologies and solutions, mainly deployed within enterprises, to deal with the storage, processing, disclosure and disposal of users' identities, their profiles and related sensitive information." (Baldwin, Mont and Shiu, 2007, p. 2).

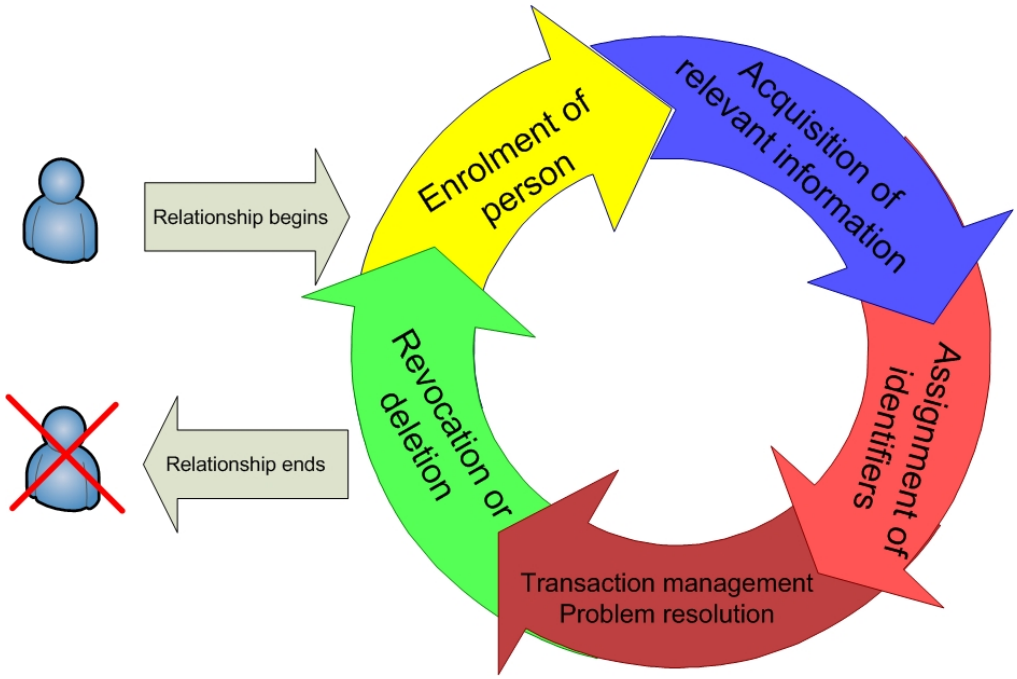
In a slightly different formulation, a report by the US National Science and Technology Council (2008, p. ES-1) defines identity management as:

> "… the combination of technical systems, rules and procedures that define the ownership, utilization, and safeguard of personal identity information. The primary goal of the Identity Management process is to assign attributes to a digital identity and to connect that identity to an individual."

Ann Cavoukian (2006, p. 5), Information and Privacy Commissioner of Ontario, offers a reduced but related definition: "in its broadest sense, [identity management] refers to the administration and design of identity attributes, credentials, and privileges." Finally, Hansen, Schwartz and Cooper (2008, p. 38) define it as "programs or frameworks that administer the collection, authentication, or use of identity and information linked to identity."

The above definitions all include the management of identity – others would say of *partial* identities – and information that relates to the human subject, such as attributes, identifiers, privileges and 'sensitive information.' These frameworks, therefore, manage the relationship between people and data about them, for the purposes of the subject and others. Identity management is concerned with the 'lifecycle' of digital identities: enrolment of the person, acquisition of relevant information, assignment of identifiers, management of transactions and problem resolution, and revocation or account deletion. Figure 4.2 below illustrates the lifecycle.

Figure 1.2 The identity management lifecycle



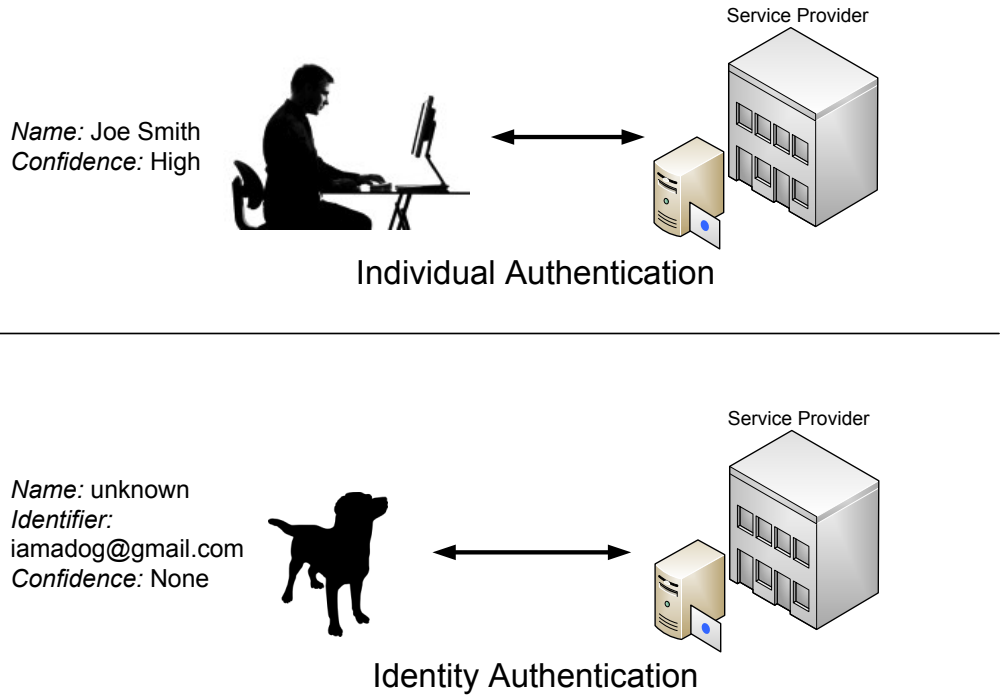
Source: adapted from Programming4Us, 2010

A key feature of IDM systems is 'authentication,' the verification of an identity or attribute claim. The most common example of authentication is when a person logs into her account on a computer system. The person claims to be a specific human being in order to access the resources assigned to her and her alone. The claim must authenticated – the truth of it must be ascertained. The US National Institute of Standards and Technology (2011, p. vi) states: "Electronic authentication … is the process of establishing confidence in user identities electronically presented to an information system." The language of 'establishing confidence' demonstrates that the truth of an identity claim need not be binary; there may be greater and lesser degrees of confidence in the claim. This point is a critical feature of US identity management policy, and is explored at length in Chapter 5.

A claim can be interchangeably called an 'assertion' – the subject asserts his identity or an attribute ('I am Gilad Rosner. I have security clearance.') The types of authentication most relevant to this research are 'individual authentication' and 'identity authentication':

> "Individual authentication is the process of establishing an understood level of confidence that an identifier refers *to a specific individual*.
>
> Identity authentication is the process of establishing an understood level of confidence that an identifier refers *to an identity*. The authenticated identity may or may not be linkable to an individual." (Kent and Millet, 2003, p. 2, emphasis added)

Figure 4.3 Individual authentication versus identity authentication



The figure above illustrates the two authentication types. In referring to '*an* identity,' this second definition embraces the partial identity concept. The distinction between the two types of authentications is the former links to a specific, known human, and the latter verifies an identity claim but the

verification need not contain sufficient information to reveal the identity of one specific person – it verifies that the claimant is the 'owner' of the partial identity being asserted. This distinction becomes more important later, but for the moment, the key idea here is that authentication answers the question, "Are you who you say are?"

The mechanism of authentication is a 'credential': "An object or data structure that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a [person]" (National Institute of Standards and Technology [NIST], 2011, p. 8). A 'token' is:

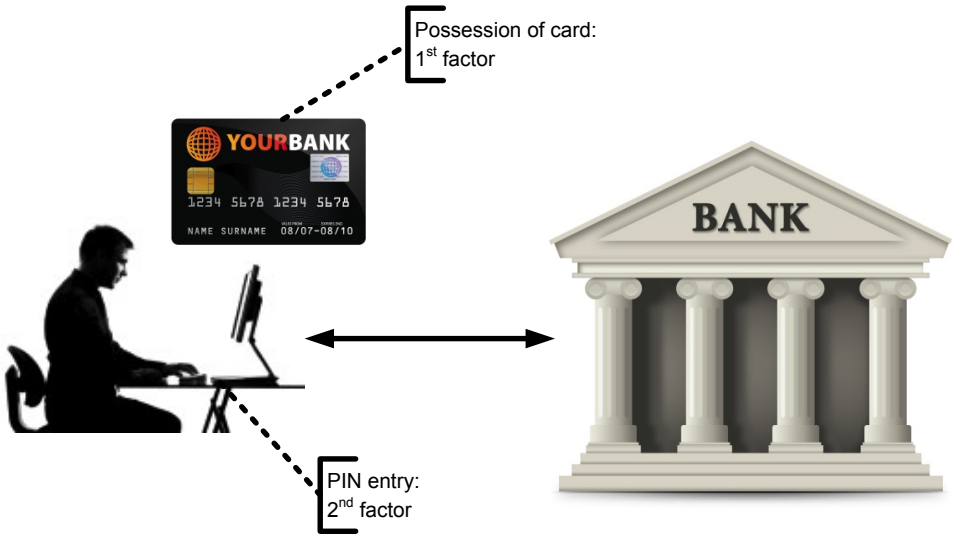
> "Something that a person possess and controls (either a unique physical object or secret data or information) that is used to authenticate his or her identity (such as a secret password, PIN, cryptographic key, ATM card, USB token, etc.). Tokens are physical devices or electronic records designed for use in authentication systems and/or to hold authenticating information." (American Bar Association Identity Management Legal Task Force, 2012, p. 44)

In this research, the term 'credential' will subsume the concept of tokens. The most widely known credential is a username and password. For example, when a person wishes to access an email service, he or she has an account with the email provider. The data comprising the account that ties it to the unique person is a partial identity. The person's username is the identifier. To prevent unauthorised people from accessing the account, a password is assigned. The username and password in combination are the person's credential. By entering the username and password ('logging in') the person authenticates that she is the appropriate subject identity. This very basic model is the origin of transactional digital identity (OECD, 2007, pp. 41-42).

In recent years, passwords have been seen as insecure, and so a second 'factor' of authentication has become a regular feature of identity management systems. Besides a password, a person may have to enter a special code he receives on his phone at the time of login, or perhaps supply a fingerprint. As

such, there are three specific methods (factors) for authenticating someone; three things one possesses: Something you *know*, something you *have*, and something you *are*. Something you know is a secret, like a password or a PIN. Something you have is a physical object, such as a bank card, radio transceiver or a key fob that produces special codes. Something you are is a unique physical attribute, like fingerprints, vein patterns or the structure of the iris – these are known as 'biometrics.' A common two-factor authentication is the use of a bank card: possession of the card (have) and the entry of a PIN (know) yields access. This interaction is depicted in the figure below.

Figure 4.4 Two-factor authentication



The German e-ID is identical to a bank card in this respect. In addition to possessing the card, to use the data it holds the citizen must enter a six-digit PIN. With regards to US citizen credentials, requirements vary, but the most common credential in use is a username and password. However, the US policy infrastructure makes provision for two-factor authentication as online interactions become more sensitive. US and German credentialing models are detailed in Chapters 5, 6 and 7. Little academic literature on US citizen credentialing exists (Adjei, 2013; Katzan, 2011a, 2011b; Schwartz, 2011). Part

of the contribution of this thesis is an in-depth examination of its history, technical models and institutional dynamics. A number of publications explore German credentialing (Hornung and Schnabel, 2009; Noack and Kubicek, 2010; Bender, Kugler, Margraf, and Naumann, 2010; Zwingelberg, 2011; Poller, Waldmann, Vowé and Türpe, 2012), but examination of the institutional factors of its privacy architectures is less common (Noack and Kubicek, 2010) and none compare directly to non-European cases.

This thesis shall use the following definition for identity management: *Identity management (IDM) is an operational and technical framework that defines and administers the lifecycle, use and security of digital identities. Authentication and the management of credentials are key focuses of IDM systems. They are transactional, and operated by organisations.*

A key finding of this study is the definition of 'identity management policy,' in the sense of public policy. The empirical data chapters (5 and 6) and the analysis in Chapter 7 provide critical data and context to validate this definition, but it is appropriate to include it here: *Identity management policy is the set of laws and policies enacted by governments and supranational bodies concerning the facilitation, procurement, use, liability, legal nature, interoperability, technologies, risk methodologies, lifecycle and privacy of digital identities for its citizens and employees. This includes physical and logical authentication, e-signature, and electronic identification technologies for access to physical and electronic resources.*

What is federated identity?

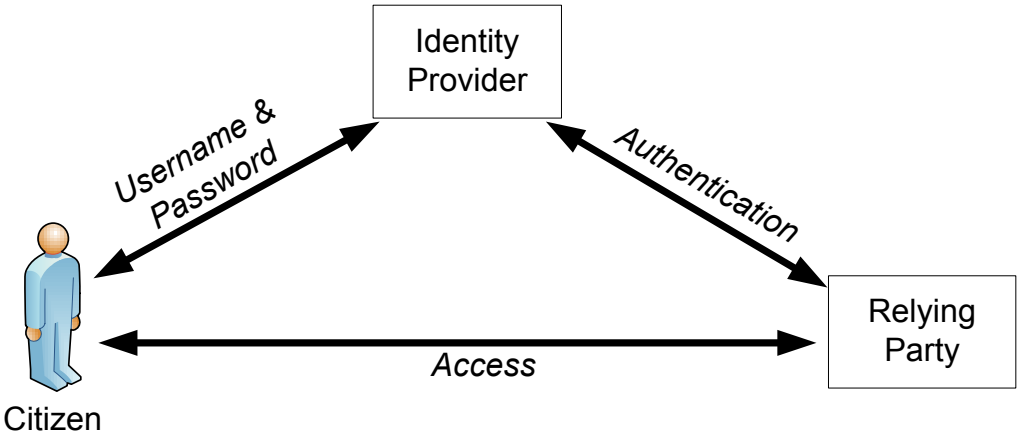
People authenticate themselves to computer systems in order to gain access to resources, such as email, file storage or the myriad services one can use online. The basic model of logging in with a username and password described above would classically occur between a person and a single service or organisation,

such as an email provider. As the internet grew from a research and university tool to a ubiquitous technology accessed by hundreds of millions of people around the world, the number of websites and other resources grew commensurately. So, too, did the number of passwords each person needed to remember; every new service requiring a user to create an account also required a password. By the late 2000s, individual users had acquired an unwieldy, large number of passwords to use across a multitude of websites (Florêncio and Herley, 2007).

In enterprise and campus computing, the 'single sign-on' (SSO) model appeared. Companies and universities had multiple, distinct services within their networks. It became more efficient for single user accounts to be used across them. The model was extended to services external to the network. For example, universities subscribe to academic publishers. An SSO model allows university members to use their local network login to access the publisher's (external) resources. To harmonise this kind of network access among the parties, a standard called Shibboleth (Shibboleth, n.d.) is used to specify the technology configurations needed to connect disparate organisations.

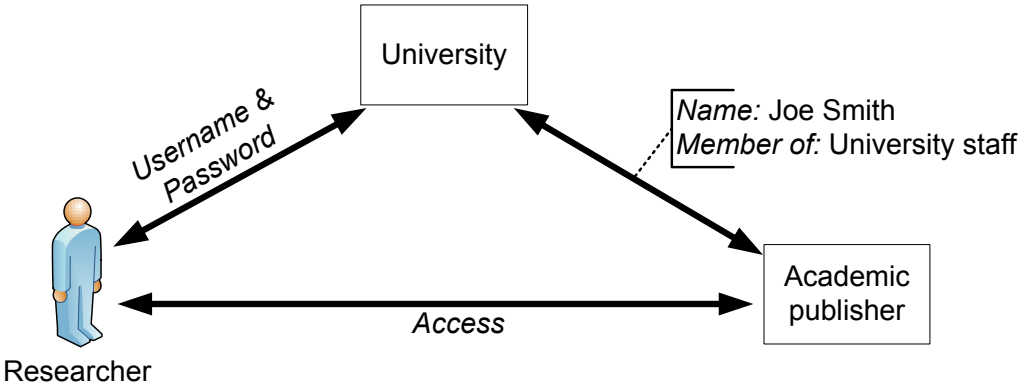
The use of identity information from one source to access a separate, disparate, or external resource is called 'federated identity' – identity information is federated across multiple organisations. In the model described above, the university is the source of identity information about its members. Each student, researcher or other staff member has an account on the university's network. That account, or login, is then used to sign on to the resources of an external organisation. The university is the 'identity provider' (IDP), and the external organisation is the 'relying party' (RP) – they rely on the identity assertion of the IDP. The diagram in the figure below shows a simplified model of federated identity.

Figure 4.5 Federated identity



This model is useful and efficient because it allows RPs to avoid the costs and labour of building and maintaining their own authentication infrastructure. Also, it lets users take advantage of having a single sign-on, reducing the number of passwords they must remember. With the federated identity model, identity claims can be exchanged as well as attribute information. For example, in the university model, the name of a researcher could be passed to an external resource as well as an attribute indicating that the person is an employee of the university. The figure below illustrates this interaction.

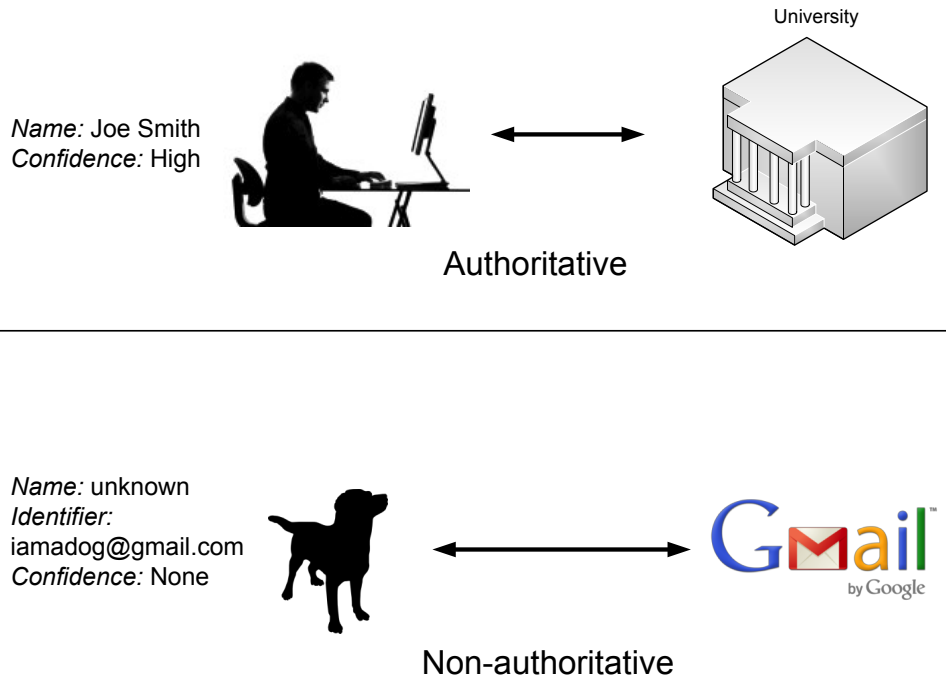
Figure 4.6 Federated identity: university and publisher relationship



Identity federation is built on various technical standards. Shibboleth is based on the Secure Assertion Markup Language (SAML) (Shibboleth, n.d.), as are a majority of commercial federation products (OASIS, 2013). A popular but now largely disused standard called OpenID was the basis of many early federation implementations (Maler, 2011). The original OpenID standard is being replaced by OpenID Connect, a substantially different technology (OpenID Foundation, n.d.). Facebook Connect is a proprietary technology that allows millions of websites to accept the Facebook login – this is the largest consumer federation service in existence (Gigya, 2013). Part of the contribution of this research is demonstrating that standards development organisations are institutional actors in the realm of privacy and data protection. IDM technologies reflect the capabilities of their underlying standards, which in turn reflect the norms, values and choices of their developers. Where policy is reliant on standardised technology, standards and their connected communities of practice can assist or hinder policy goals. This theme is explored in Chapter 8.

Many internet services do not require people to validate their identities when they sign up. In the case of a free service, such as the popular email services Gmail and Yahoo! Mail, people do not need to provide proof of their identity when creating an account. Both providers have federated their logins with OpenID, meaning that relying parties who accept OpenID logins can use Gmail and Yahoo! Mail accounts despite the fact that those accounts are not 'authoritative.' That is, the identities 'bound' to the logins (credentials) have not been 'proven' or 'vetted,' i.e., corroborated. Contrast this with university logins. Universities must know definitively who their members are because they have a closer relationship: they are providing regulated services, maintaining long-term records, and are billing them. Accordingly, there is higher confidence that a university login is authoritatively bound to a specific person. Figure 4.7 below illustrates these identity relationships.

Figure 4.7 Authoritative versus non-authoritative identity relationships



Returning to the Kent and Millet (2003) definitions above, a university login that is authoritatively bound to a person can be used for 'individual authentication'; the process authenticates a specific human. Authentications with an unproven Gmail account are 'identity authentications'; the credential is authenticated, but not the underlying human. The issue of authoritative credentials is key in the US empirical research, and will be explored further in that chapter and the Citizen Credentialing section below. In Germany, their e-ID credentials are strongly bound to the intended human by secure, state-based processes, so any claims based on the e-ID are considered authoritative.

The ID spectrum

The distinction between authenticating an identity versus authenticating a specific person leads to a discussion of the ID 'spectrum' (Clarke, 1999). There

are three main forms of identification: anonymous, pseudonymous and identified.

Figure 4.8 The ID spectrum

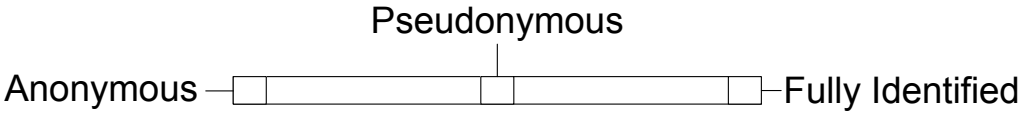


Figure 4.8 above depicts the ID spectrum. There is no widely accepted term for 'fully identified' that sits easily within the spectrum, though two experts (Maler and Reed, 2008, p. 18) have trialled the word "veronymous"; it is aesthetically superior to the word, "absonymous," proffered by the European Network and Information Security Agency (2011, p. 10). Broadly stated: "The concepts of identification and anonymity are extremes on a continuum of degrees and modes of identifiability and non-identifiability" (van der Hof, Leenes and Fennell, 2009, p. 41).

Anonymity, the state of being anonymous, means that no information can be tied from a message or other transactional data to its source. Clarke (1999, orig. emph.) defines it as such: "**An anonymous record or transaction** is one whose data **cannot** be associated with a particular individual, either from the data itself, or by combining the transaction with other data." There are degrees of anonymity (see Kling, Lee, Teich and Frankel, 1999), but the above definition is appropriate for this research.

Pseudonymity is at the root of a famous 1993 New Yorker cartoon (Steiner, 1993):

"On the Internet, nobody knows you're a dog."

Clarke (1999, orig. emph.) usefully defines pseudonymity:

> "**A pseudonymous record or transaction** is one that **cannot, in the normal course of events**, be associated with a particular individual.
>
> Hence a transaction is pseudonymous in relation to a particular party if the transaction data contains no direct identifier for that party, and can only be related to them in the event that a very specific piece of additional data is associated with it. The data may, however, be indirectly associated with the person, if particular procedures are followed, e.g. the issuing of a search warrant authorising access to an otherwise closed index.
>
> To be effective, pseudonymous mechanisms must involve **legal, organisational and technical protections**, such that the link can only be made (e.g. the index can only be accessed) under appropriate circumstances."

This thesis will use the above definition for pseudonymity. Anonymity is a rare condition on the internet, though pseudonymity is commonplace. The

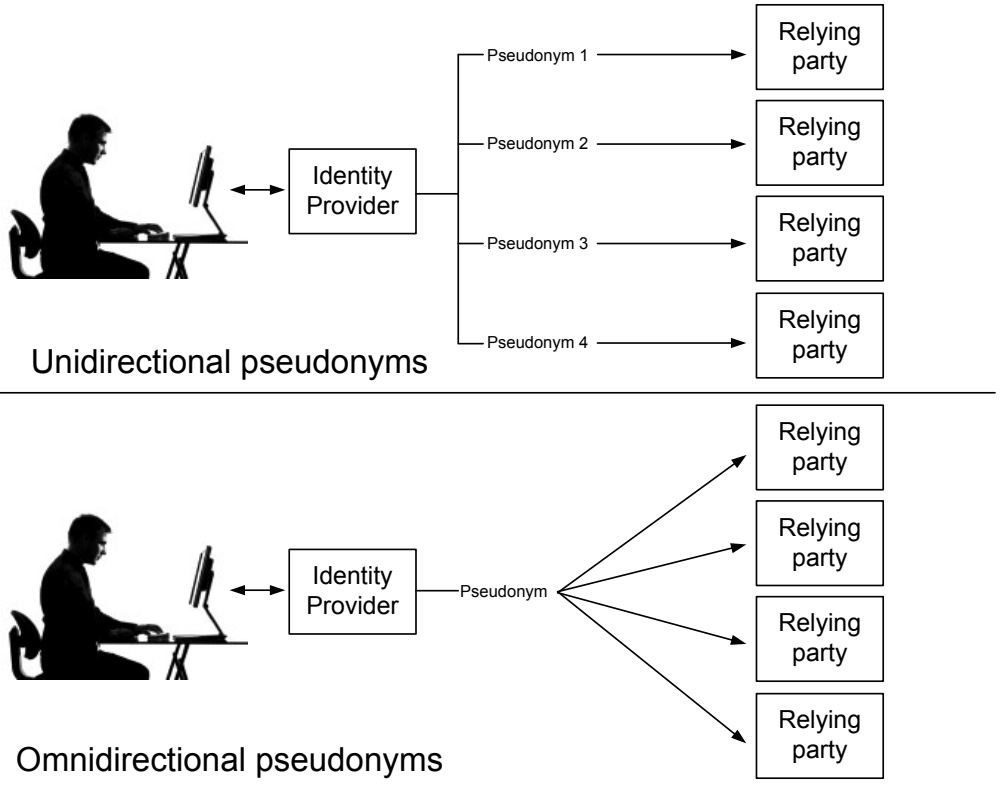
distinction between individual authentication and identity authentication is pertinent – uncorroborated Gmail accounts that do not include a person's name in the username are pseudonymous. They are not anonymous because Google, the owner of Gmail, or a law enforcement agency could potentially tie a username to an individual computer, and thereby its human operator, by its IP address or through other means. Pseudonymity is a vital element of unlinkability, discussed below. The 'legal, organisational and technical protections' Clarke cites are the substance of the privacy and data protection policies this research examines. Through this lens, the thesis is an analysis of national pseudonymity policies.

The other pole of the spectrum, fully identified, means that the identity of a unique person is known. A common example of full identification is online banking. Banks must not grant financial record access to unauthorized people, so they operate credentialing systems that unambiguously identify people when they log in. This is another illustration of an organisationally governed partial identity: banks enrol the customer, assign an identifier, bind it to a credential, and grant it access to sensitive information.

Any identifier that does not contain a name or other 'linkable' attribute, such as a social security number or phone number, can be considered pseudonymous. In the venerable Gmail example, any username that does not contain a full name, e.g., Univac1234@gmail.com, is a pseudonym. In a federated identity system, IDPs assert identities to RPs by sending an identifier of the subject identity. For IDPs who have vetted the underlying subject identities, such as a university or a medical facility, they have the option of sending veronymous identifiers that disclose the full identity of a person, or pseudonymous identifiers. The choice may be based on the commercial relationship between the IDP and the RP, may be regulated by privacy laws, or both. For example, the US Drug Enforcement Agency requires that doctors who login to electronic

prescription services be bound to high confidence credentials that contain fully identifying information (Privacy and Security Tiger Team, 2012). In other cases, an IDP may send a pseudonymous identifier to an RP without further information that could identify the underlying person. More importantly, an

Figure 4.9 Unidirectional versus omnidirectional pseudonyms



IDP can send a different pseudonymous identifier to each relying party in order to frustrate profiling of a user's activity.

These different pseudonyms are called 'unidirectional,' versus single pseudonyms used across all transactions which are called 'omnidirectional.' Figure 4.9 above illustrates the distinction. If a phone number was used as an identifier in all cases, it would be an omnidirectional pseudonym. It would be linkable because it would link all of a user's online activities, and could

potentially reveal the underlying subject's identity with relative ease. Unidirectional pseudonyms are key to unlinkability, and feature prominently in the technical architectures of Germany and the US.

What is unlinkability?

One international standard, ISO/IEC 15408-1 (2009, p. 78) defines unlinkability as follows:

> "[Unlinkability] ensures that a user may make multiple uses of resources or services without others being able to link these uses together…. Unlinkability requires that users and/or subjects are unable to determine whether the same user caused certain specific operations in the system."

Marit Hansen (2012, p. 24) relates unlinkability to 'privacy-relevant data':

> "Unlinkability aims at separating data and processes: This means that processes must be operated in such a way that the privacy-relevant data are unlinkable to any other set of privacy-relevant data outside of the domain. If full unlinkability cannot be achieved, it should be realized to the extent that linking would require disproportionate efforts for the entity establishing such linkage."

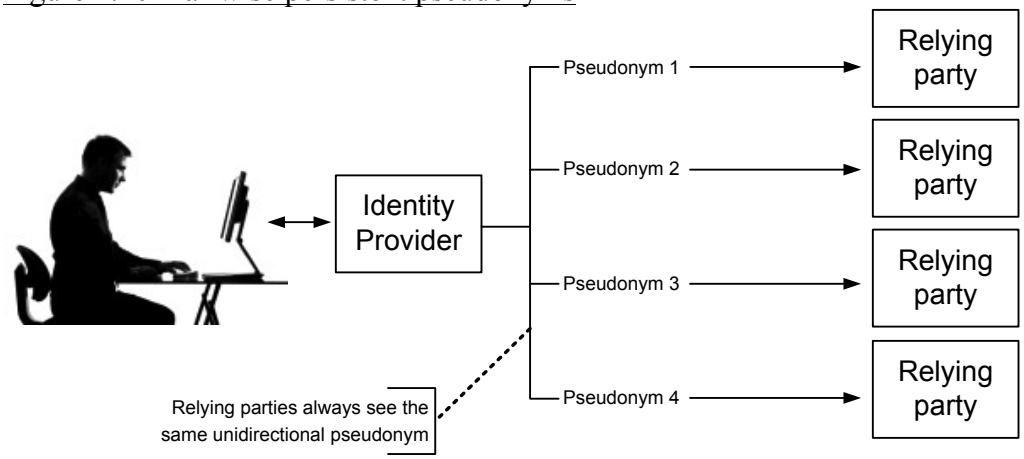
These 'disproportionate efforts' are another face of Clarke's (1999) 'legal, organisational and technical protections.' Unlinkability's opposite, 'linkability,' can therefore be defined as follows:

> "Linkability of two or more items of interest (… e.g., subjects, messages, actions, ...) from an attacker's perspective means that within the system … the attacker can sufficiently distinguish whether these [items] are related or not." (Pfitzmann and Hansen, 2010, p. 12)

This thesis shall use the following definition for unlinkability, largely absorbing ISO/IEC 15408-1: *Unlinkability is the intentional severing of the relationships ('links') between two or more data events and their sources, ensuring that a user may make multiple uses of resources or services without others being able to link the uses together.*

The central mechanism of unlinkability is pseudonymity. As described above, a single pseudonym used across multiple contexts is called 'omnidirectional,' whereas the use of a different pseudonym for each transaction is called 'unidirectional.' Omnidirectional pseudonyms are susceptible to profiling because of the linkability created via identical identifiers. That is, if the same identifier – for example, an email address – is seen across multiple uses, and all of the uses are visible to a single organisation, all uses can be put in the same profile keyed to the identifier. If that pseudonymous identifier becomes tied to the real-world person, a profile of all those uses is then associated with one specific person. On the other hand, if each online activity is keyed to a separate unidirectional pseudonym, profiling is not possible via the identifier.

Figure 4.10 Pairwise persistent pseudonyms



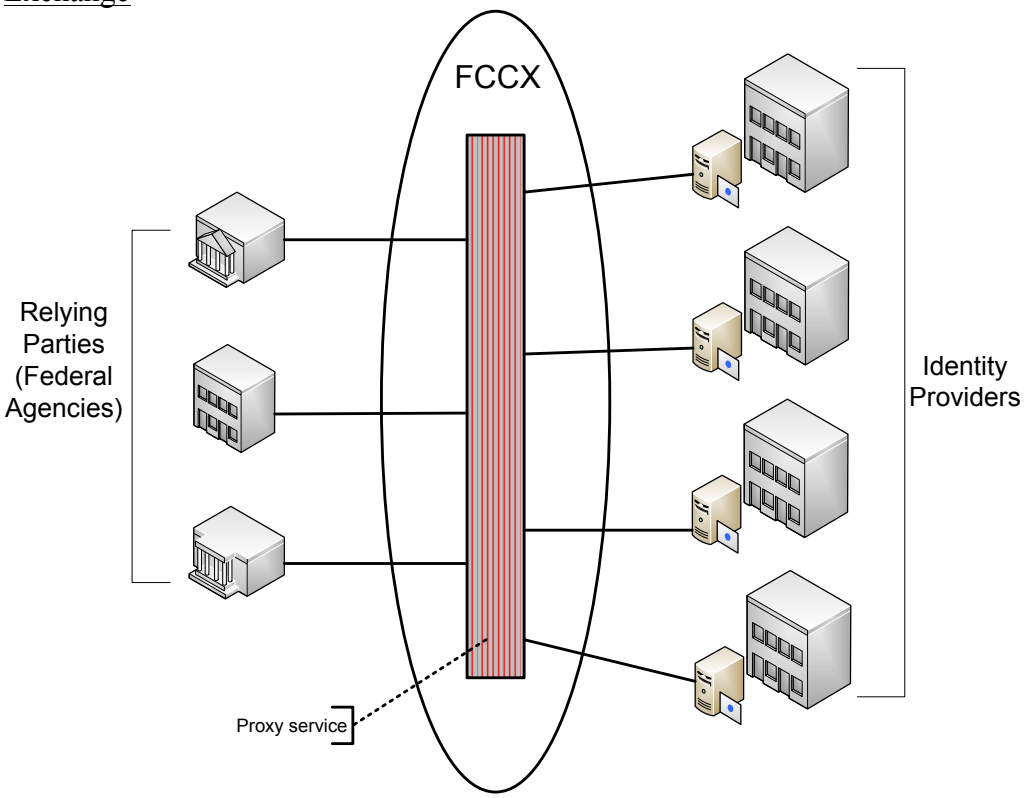
In federated identity systems, a common configuration is the use of a single pseudonym for each relying party (rather than for each session or transaction) – these are called 'pairwise persistent' pseudonyms, depicted in Figure 4.10 above. In this arrangement, each relying party sees the same pseudonym each time, allowing it to recognise the user on return visits.

This also means that the identity provider maintains a mapping of each persistent pseudonym pair between the user and the RP. If multiple RPs collude, in the absence of other linkable information, such as a credit card or

phone number, they should not be able to correlate the disparate activities with a single person. This can be termed, 'RP/RP blindness' – relying parties are blind to one another. However, collusion between multiple RPs and the IDP would connect the activity to one person because the IDP maintains the mapping. For US citizen identity management, this is the current technical arrangement; it is explored in Chapters 5 and 7.

An alternative strategy to the above configuration is to insert a third party between IDPs and RPs – a 'proxy.' In theory, an IDP can send a pairwise persistent pseudonym to an RP, but the identity of the RP is masked by the proxy receiving the user pseudonym from the IDP. The proxy then removes information that identifies the IDP, matches the credential request to the correct RP, and sends the credential on. This arrangement can be termed 'IDP/RP blindness,' and it is a stated goal of near-term US identity management policy, detailed further in Chapters 5 and 7. Figure 4.11 below shows a simplified illustration of the Federal Cloud Credential Exchange (FCCX), which is intended to support IDP/RP blindness. Accomplishing this while making such a system auditable and secure is the subject of expert debate (John, 2012; Hare and Woodhill, 2013) and success is not yet a foregone conclusion.

Figure 4.11 Federated identity with a proxy: the US Federal Cloud Credential Exchange



The German e-ID system creates a third variant. In that architecture, there is no identity provider *per se*. The e-ID card itself serves that function – identity information, attributes and pseudonyms are all sent by the card when a user consents. When citizens login to sites pseudonymously, RP/RP blindness is the result, but the credential issuer, the German government, is never aware of credential uses. This makes the system 'unobservable' to the issuer; the card never reports or records its activities. This is an intentional policy choice, analysed in Chapters 6 and 7.

Unlinkability serves a number of privacy and data protection goals. Chief among these is the frustration of profiling: "Unlinkability technically prevents (illegitimate) merging of profiles by linking them" (Bhargav-Spantzel,

Camenisch, Gross, and Sommer, 2007, p. 500). It is thereby a means to realise the classic data protection principles of data minimisation, purpose specificity and use limitation (OECD, 1980; U.S. Department of Homeland Security, 2008). The ULD, a German data protection authority, writes:

> "Unlinkability is the key element for data minimisation because it encompasses all kinds of separating data from persons, e.g., by means of anonymisation, pseudonymisation, erasure or simply not having the data at all…. The overarching objective of this protection goal is to minimise risks to the misuse of the privacy-relevant data and to prohibit or restrict profiling spanning across contexts and potentially violating the purpose limitations related to the data." (Zwingelberg and Hansen, 2011, p. 247)

Much academic literature on privacy has embraced the view that privacy is contextual (Prins, 2006; Waldo, Lin and Millet, 2007; Hansen, Schwartz and Cooper, 2008; Lips, Taylor and Organ, 2009a, 2009b; Nissenbaum, 2010). That is, a respect for the privacy of individuals takes into account the contexts in which information about them is shared. There are norms associated with those contexts, and it is a violation of privacy to transgress those norms by commingling contexts inappropriately (Nissenbaum, 2010). Identity management literature has incorporated this view:

> "**Identity is contextual.** People have different identities that they may wish to keep entirely separate. Information can be harmful in the wrong context, or it can simply be irrelevant. Keeping identities separate allows a person to have more autonomy." (OECD, 2007, p. 26)

Unlinkability is a strategy to maintain separation between contexts, contributing to 'linkage control': "In the digital world full of identifiers for digital identities which often can easily be linked, better linkage control by individuals is crucial for maintenance of their private sphere" (Hansen, 2008, p. 1591). The issue of control is fundamental to 'informational self-determination,' a right derived by a 1983 German Constitutional Court that is fully detailed in Chapter 6. Briefly, this right confers, among other things, a wide latitude of control over information about oneself in service of dignity

and the ability to fully develop one's personality. In German identity management policy, unlinkable credentials are part of a broader strategy to ensure informational self-determination. In the US, they are more directly connected to data minimisation goals. Both strategies serve a bias against profiling.

Other recent considerations of privacy and data protection, such as Cameron's (2005) "Laws of Identity" and the broad spectrum of work on 'privacy by design' (Cavoukian, 2006; Rost and Bock, 2011) espouse additional principles which unlinkability addresses. Cameron's (2005, p. 8) Laws specifically call for "Directed Identity": "A universal identity system must support both 'omnidirectional' identifiers for use by public entities and 'unidirectional' identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles." Unlinkability aids 'user-centricity' goals, which seek to place the concerns and control of users at the centre of identity management architectures (Bhargav-Spantzel, et al., 2007). The privacy goals and strategies served by unlinkability underpin, in explicit and tacit ways, the IDM policies of Germany and the US.

Citizen Credentialing

The issuance or facilitation of identity credentials by and for the state is directly linked to larger discussions about national identification projects. This subject, covered in great depth by Torpey (1997, 2000, 2001), Caplan and Torpey (2001), Lyon (2009), Bennett and Lyon (2008), Lips, Taylor and Organ (2009a, 2009b), van der Hof, Leenes and Fennell (2009), Whitley and Hossein (2009), Kerr, Lucock and Steeves (2009), and the London School of Economics (LSE Systems and Information Group, 2010) provides a rich backdrop for discussions about the social dimensions of online credentials. Most of this literature follows identity cards and papers and their related systems. The German case study of this thesis can connect to these larger

discussions as their online credential is a function of their e-ID card, issued in 2010 to replace the prior paper card. But the US case study is unanchored to physical ID cards, relying instead purely on software and its underlying infrastructure. There is a gap in identity literature of policy analyses of non-card-based identity credential systems; the US cases addresses this. The research as a whole adds to information policy scholarship by analysing the privacy architectures of specific countries' authentication infrastructures. There is a general lack of empirical research on US citizen credentialing efforts, which this thesis addresses.

Identity systems help states to 'embrace' their citizens (Torpey, 1997); they make people 'legible' (Scott, 1998). James Scott (1998, p. 183) writes:

> "Legibility is a condition of manipulation. Any substantial state intervention in society … requires the invention of units that are visible. The units in question might be citizens, villages, trees, fields…. Whatever the units being manipulated, they must be organized in a manner that permits them to be identified, observed, recorded, counted, aggregated, and monitored."

The identity scholars noted above examine the harmful and beneficial sides of this embrace. Identity papers – more so electronic ones – enable broad and deep surveillance. John Torpey (1997, 2000, 2001) argues that identity papers and passports are administrative instruments to help states expropriate the legitimate means of people's movement. They help determine 'who is in and who is out' for purposes of control and, more germanely, who can access the benefits of the state. In addition to issues of movement and surveillance, identity documents facilitate access to public services. To ensure that the 'right' people are receiving services – only those eligible and the finer gradations of which particular service – public agencies must know with whom they are transacting. For in-person services, traditional paper documents usually suffice. But, for e-government, discussed further below, transactions take place remotely. Paper documents cannot be used to authenticate people at

a distance as there is no way to compare photos to the presenter, and anti-counterfeiting measures are defeated when the documents are photocopied or scanned.

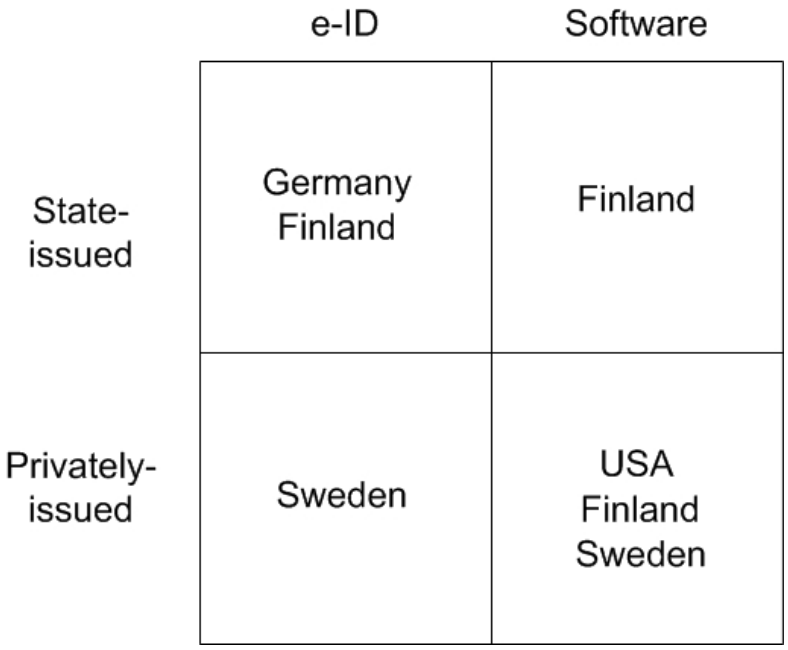
In the two research cases, online credentials were developed in the context of electronic government services. In the US, a completely new set of policies had to be created for the government to plan to credential the whole of its populace. In Germany, the e-ID was borne of their prior national ID, adding features to allow citizens to authenticate online. In the policy development of both, the authentication needs of e-government were cited as central motivations (Schmidt, 2005; ULD, Interview; G001, Interview; G003, Interview). Also in the two cases was an explicit wish to enable 'trustworthy transactions' online, both for the benefit of individuals and the internet as a whole (White House, 2011; Möller, Interview). While there is much discussion in literature of the surveillance of citizens via electronic identity management systems, there is very little of government policies encouraging strong authentication for general benefit. The empirical work of this thesis contributes to the multi-faceted discussions of IDM by analysing specific attempts by government to both engender online trust and shut its panoptic eye to its citizens' online activities.

Electronic government (e-government) is the use of electronic resources by government for its own internal processes or for the delivery of public services. The main goals for the introduction and expansion of e-government are cost savings, efficiency and greater engagement with relevant populations. Examples of e-government include online tax form submission, application for financial benefits, payment of fines, submission of medical information, obtaining court documents, consumer complaints, and participation in the political process (West, 2007). Many meaningful e-government services involve an exchange of personal information. In Germany, the US and many others, laws and policies that dictate fair and appropriate collection and use

govern the exchange of personal data. Governments must ensure that they do not release personal data to unauthorised people. Correspondingly, when they transact with their populaces online, agencies must have high confidence that a claimed identity is authentic. Citizens and other 'customers' of public services therefore must be bound to identity credentials that agencies can rely upon.

Online credentials make people legible in the electronic world. There are two forms of digital citizen credentials: hard and soft. That is, a physical credential – for this research, an electronic identity card – and an intangible one based on software or 'certificates' (trusted documents written in computer code). There are also two types of credential issuers: the state and private actors. These forms and issuers can be represented as a matrix:

Figure 4.12 Matrix of credential type and issuance



Germany and the US are the two cases of this research, but Sweden and Finland are included for comparative, explanatory purposes. The upper left box, state-issued e-ID, contains countries where the state itself issues a plastic

card that contains an electronic chip. The chip holds the bearer's identification and attribute data, such as name, date of birth and residential address. The card also has a capability to authenticate the bearer online to e-government services. The German e-ID is a member of this group; the card's genesis and features are described fully in Chapter 6. Another member is Finland, whose government issues FINEID, a national identity card that can be used online (Rissanen, 2010). The lower left box, privately-issued e-IDs, are identical to the box above except that the issuer is a private organisation. In this box is Sweden, whose citizens can obtain e-IDs in card form from Swedish banks and a telecommunications company (Grönlund, 2010). These privately-issued cards can be used to authenticate the bearers to e-government and private services. The box in the upper right, state-issued software-based IDs, contains countries whose states issue trustable certificates for use in authentication. Finland also occupies this box because the Finnish government issues citizen identification certificates that can be downloaded into mobile phones (Stevens et al., 2010, p. 23; Valimo, n.d.). The lower right box, privately-issued software-based IDs, contain countries whose citizens can use software or certificates issued by private organisations to access e-government resources. The US falls into this category; the technical and policy models are fully explained in Chapters 5 and 7. Finland and Sweden are also members of this group as both countries' citizens can obtain downloadable certificates issued from banks to authenticate themselves online. As the four country examples illustrate, citizen credentialing can be publicly managed, privately managed, or a combination of both.

It is valuable to consider two other dimensions – longevity and whether credentials are compulsory. In the case of physical e-IDs, longevity becomes a factor because ID cards have finite lifespans. Also, the validity length of national ID cards may be specified by law, as in the case of Germany which requires a 10-year document life (Noack and Kubicek, 2010). This constraint

forced Germany down a path of using 'contactless' (RFID) technology. Longevity is not a consideration for soft credentials as there is no physical document to 'wear out.' Validity of a certificate may still be a factor, and a renewal period may be instituted. The US, which relies exclusively on privately-issued soft credentials does not institute a maximum validity requirement.

The other consideration is whether a citizen must possess a credential by law. In Germany, citizens must hold either a national ID card or a passport from age 16 onwards (Noack and Kubicek, 2010). This requirement means that all German citizens will hold either an e-ID or a passport by 2020, when all prior national IDs will have expired. However, activation of the online authentication feature of the e-ID is voluntary. As Chapter 6 details, only 28% of German citizens have elected to activate the feature (Bundesverwaltungsamt, 2013). Voluntariness is also a critical characteristic of US credentialing in accordance with Americans' strong antipathy towards national identification schemes. As the US data chapter shows, national identity management policy documents explicitly disavow kinship with a national ID.

Conclusion

This chapter has reviewed key terms and concepts necessary for an examination of the appearance of unlinkability in national identity management policies. Identity management products, protocols and systems are being built with unlinkability features to comport with existing laws and policies, in service of the norms and values of relevant communities of practice, and to include features believed to be desirable to customers. Unlinkability is a member of the group known as 'privacy-enhancing technologies', though it is often accomplished through a combination of both technical and social enforcement mechanisms. This research explores the spectrum of enforcement

arrangements possible with unlinkable credential systems in the two empirical data chapters. Unlinkability is defined not by its method, though, but by its goals: to separate contexts and uses, and give users greater control over the sharing of identifying information and their online activities.

The appearance of unlinkability in national policies is a recent phenomenon. No academic policy literature specifically gathers empirical case data on unlinkability policies. There is no literature that examines its institutional factors, and there is limited literature that situates unlinkability in larger analyses of extant information policy. This research addresses these gaps, gathering a rich body of empirical data to particularise the evolution of privacy interests in two countries. These are not only instrumental case studies (Stake, 2005, p. 445), examining new, noteworthy phenomena. This research is important because it traces government activity to adapt data protection principles in light of rapid changes in technology. Public policy is notoriously out of step with technological change (Reidenberg, 1997). This thesis finds that governments and their agents have been considering the sensitivity and impact of identity management technologies alongside their swift evolution. The empirical data shows a great degree of collaboration between policy-makers, academics, technologists, and businesspeople to develop IDM policy. These processes are technocratic given the level of technical detail needed to understand the tools available to achieve policy goals; the processes are both iterative and not guaranteed of success. This thesis contributes to the study of information policy by connecting historical trends in data protection and privacy and their underlying principles to contemporary discussions of digital identity and its capacity to be regulated. It highlights the interplay of policy-making, technical standards and business interests leading to the multi-stakeholder processes that yielded modern identity management policies and their embedded privacy choices. The research unites US and European identity

management concepts, lexicons and technical designs which have so far not been directly compared.

The key definitions for the present research are as follows:

Digital identity	Digital identity is a set of information and attributes that can disaggregate a person from all other persons within a given context. It is transactional and composed of data, and is represented by an identifier which may or may not reveal the full identity of the underlying person.
Identity management	Identity management (IDM) is an operational and technical framework that defines and administers the lifecycle, use and security of digital identities. Authentication and the management of credentials are key focuses of IDM systems. They are transactional, and operated by organisations.
Identity management policy	Identity management policy is the set of laws and policies enacted by governments and supranational bodies concerning the facilitation, procurement, use, liability, legal nature, interoperability, technologies, risk methodologies, lifecycle and privacy of digital identities for its citizens and employees. This includes physical and logical authentication, e-signature, and electronic identification technologies for access to physical and electronic resources.
Federated identity	The use of identity information from one source to access a separate, disparate, or external resource is called ‘federated identity’ – identity information is federated across multiple organisations.

Pseudonymity (the state of being pseudonymous)	"A pseudonymous record or transaction is one that cannot, in the normal course of events, be associated with a particular individual. Hence a transaction is pseudonymous in relation to a particular party if the transaction data contains no direct identifier for that party, and can only be related to them in the event that a very specific piece of additional data is associated with it. The data may, however, be indirectly associated with the person, if particular procedures are followed, e.g. the issuing of a search warrant authorising access to an otherwise closed index. To be effective, pseudonymous mechanisms must involve legal, organisational and technical protections, such that the link can only be made … under appropriate circumstances." (Clarke, 1999, emph. removed)
Unlinkability	Unlinkability is the intentional severing of the relationships ('links') between two or more data events and their sources, ensuring that a user may make multiple uses of resources or services without others being able to link the uses together.
E-government	Electronic government (e-government) is the use of electronic resources by government for its own internal processes or for the delivery of public services.

CHAPTER 5: UNLINKABILITY IN US INFORMATION POLICY

Introduction

This chapter details empirical research into the federal privacy and data protection policies of unlinkability in the United States. The first part of the chapter is a chronology of the federal government's efforts to obtain digital identity credentials to enable citizens to access electronic government (e-government) resources. Several privacy goals emerged within these efforts, including an intention to build credential services that disallowed or hindered website operators and credential providers from tracking citizens' online activity.

The US was chosen as a research case for several reasons. Firstly, an initial literature review revealed evidence that unlinkability was emerging in some form within policy relating to digital identity. The US has a federal government and this policy was occurring at the federal level. This supported a most similar systems design for a comparative study with Germany. E-government and citizen identity management initiatives were occurring in a similar timeframe to Germany – the late 1990s and throughout the 2000s. A key difference between the two countries was the source of citizen credentials. The German state was supplying credentials directly to its citizens via a national e-ID, whereas the US was relying on private organisations to supply credentials to its citizens. Germany and the US both have institutionalised data protection, though it manifests differently in each country. Germany has, in line with Europe, an omnibus approach to personal data protection. The US has a sectoral approach, dividing its protective measures into data categories such as health, financial, and educational. Germany has a data protection 'layer' in the form of federal and state data protection authorities. The US has no equivalent. Nonetheless, unlinkability is appearing in both countries, in part because of

similar data protection principles – chiefly, data minimisation – at the heart of the US 'Fair Information Practice Principles' and German data protection law. See Chapter 3 for a full explanation of the methodology and case selection criteria.

The empirical data is derived from twenty-eight interviews with actors who directly influenced or were affected by unlinkability policy, plus primary documentation such as laws and official memoranda, and secondary documentation such as academic literature and commentary. Interview subjects include policy-makers; government lawyers; privacy advocates; Don Thibeau, Chairman of the Open Identity Exchange; Dazza Greenwood from the MIT Media Lab; Paul Trevithick, founder of the Information Cards Foundation; and Andrew Nash, head of identity for Google. See Appendix A for a complete list of all interview subjects.

The first section of this chapter examines the intertwining of e-government priorities and identity management policies. It details the reasons behind the government's choice to obtain credentials from the private sector rather than create them themselves, and the policy frameworks necessary to 'trust' externally-generated credentials. This includes a risk methodology federal agencies needed to judge the validity of non-federal credentials. The section examines the policy distinctions between credentials intended for e-government use, and those intended for private use. The chronology highlights the formal policy instruments and their privacy language to illustrate how unlinkability emerged in US policy.

The second half of the chapter is a discussion of the major themes that emerged from the data. The themes were derived from interviews and literature, as well as inductive analysis. Themes are selected and presented in order to highlight the key issues relevant to explaining the policy of unlinkability (McClure, et

al., 1999; Braun and Clarke, 2006). The major themes analysed are: the spectre of a national ID, the various methods of unlinkability, commercial necessities, technical versus social methods of regulation, policy comparability versus compliance, the various policy actors, and usability of IDM systems. Several of these themes appear in the analysis of German unlinkability policies, and other themes are particular to the US case due to history, law, policy constraints and culture.

Overview

In the final years of the 20th Century, the US government sought to take advantage of the burgeoning internet technologies which had begun to thrive in the commercial world. The Clinton Administration laid out several policy goals intending to re-engineer government through the use of information technology (Lips, 2000, pp. 199-204). In the early years of the succeeding Bush Administration, government administrators recognised that sound identity management was vital to successfully advancing e-government (Turning the tortoise, 2002). An endemic rejection of national identification schemes stemming from civil liberties concerns foreclosed the possibility of the government creating online credentials for the American people. The government looked to the private sector to supply the credentials needed to authenticate people when they used federal websites. That is, the US government, in line with contemporaneous activities in the commercial world, wanted their IT systems to be able to 'consume' identity credentials that were created and managed by external private sources. These private actors, in this context, are called 'identity providers'.

E-government websites are part of government IT resources and are therefore subject to federal privacy and data protection laws regarding government-held data. Comparable policies had to be enforced upon the private actors whose systems would interact with government data. This set of policies expressed a

desire to inhibit the ability of government agencies to know about people's disparate online activity, as well as to inhibit identity providers from knowing which government websites people visited; or, at least prevent them from using and sharing that information. The intentional hiding of one's online activity within the credential space – severing the links between the sites one visits – is called 'unlinkability'. See Chapter 3 for a complete overview of unlinkability.

The appearance of unlinkability as public policy is part of the larger story of the various policies and decisions made en route to government use of federated identity technologies, as well as the US government's formal pursuit of e-government. Unlinkability was part of a set of privacy and security concerns that manifested through most of the government's efforts to increase citizen participation electronically and gain benefits that the internet portended for citizen-government interaction. By relying on private actors to supply digital credentials for citizens, the US effectively outsourced the implementation of policy needed to realise its e-government goals. Private actors, however, did not see the value in meeting the government's needs for high confidence credentials. The US 'use case' of secure, high confidence, privacy-preserving credentials for its citizens is in tension with the private sector's need for a profitable 'business case.' As a result, US identity management efforts for citizens are stalled. Unlinkability, nested within these efforts, is also therefore unrealised.

Early Government Identity Federation

By the early 2000s, the federal government had begun to federate digital identity credentials among agencies across the 'Federal PKI Bridge' (G003, Interview; G004, Interview; Dazza Greenwood [Greenwood], Interview). PKI – public key infrastructure – was an established method of using cryptography to ensure that messages originated from known senders and were not tampered with en route. In this case, the messages were, among other things, 'identity

assertions', allowing a federal employee from one agency to gain access to another agency's IT resources by asserting that she was a specific, authorised person. The assertions (messages) would be cryptographically 'signed' to allow the receiving end to validate their origin and determine that they were not tampered with. Originally, the Federal Bridge only serviced federal employees; i.e., it was not for citizen access to federal resources. In 2006 the Federal Bridge cross-certified with a private service, the CertiPath PKI Bridge, serving the aerospace-defence industry, enabling federal relying parties to authenticate private sector employees at the same standards for trust as for federal employees (G004, Interview).

E-Government Priorities

As the World Wide Web came into common usage, federal agencies began to put government resources online. E-government was a political priority for the Clinton Administration (1992– 2000) and Bush Administration (2000–2008) (Lips, 2000, pp. 199-204; G001, Interview; G003, Interview; G008, Interview). The Clinton Administration believed information and communications technology to be "the essential infrastructure for the government of the 21st century" (Lips, 2000, p. 200; White House, 1993, Executive Summary). Electronic access to government resources was a critical part of this vision. The White House's 1993 report on *Reengineering Through Information Technology* stated:

> "The government must not apply information technology haphazardly or sporadically. It also should not simply automate existing practices. Instead, public officials should view information technology as the essential infrastructure for government of the 21st Century, a modernized 'electronic government' to give citizens broader, more timely access to information and services through efficient, customer-responsive processes." (White House, 1993, Executive Summary)

Towards the beginning of the Bush Administration, identity management was identified as a critical priority to progressing e-government (Turning the

tortoise, 2002). Administrators working in this policy area recognised that accepting online credentials from sources external to the government was necessary to meet the Bush Administration priorities for expanding e-government (G003, Interview). This would lead to the creation of initial policy instruments to allow government agencies to accept non-federal credentials. One administrator recalled:

> "Agencies were already trying to bring their services to the web, or to the internet, and for whatever reason were having trouble with that last mile, because the last mile's always the hardest. And so the idea was that we're going to put this together and actually help get them there." (G001, Interview)

Exposure to British Policy Models

By the early 2000s, Britain had successfully built a framework named tScheme to allow credentials created outside of government to be used to access electronic government resources (G001, Interview; G003, Interview; G008, Interview; Richard Wilsher [Wilsher], Interview). tScheme was led and managed by the private sector. Seeing similar needs in the US, federal administrators met with tScheme administrators to understand what could be similarly applied. The principal architect for this framework, Richard Wilsher, was subsequently engaged by policy-makers to advise US efforts (G001, Interview; Wilsher, Interview). Policy designs were also influenced by the British E-Envoy Office that focused on British e-government efforts, and through discussions with other countries (G001, Interview; G003, Interview; G004, Interview; Wilsher, Interview). An administrator recalled the history of tScheme and its privately-led nature:

> "So, the secret is that the whole concept for the E-Authentication Program, and then subsequently for the Trust Framework provider program, was borrowed from our friends across the pond and the tScheme program … The Envoy's office … said, 'We're going to start this national validation scheme, or certification scheme, and, industry you're invited to play.' And British industry came back to them and said, 'No, we're not going to do that. We, industry, will manage this.

> We will give you, government, a seat at the table. But we will manage this.' And the government said, 'Well alright then. We'll give you five years. We'll let you take the lead. You've got five years to make it work. If you don't make it work, we're taking it back.' They made it work. So, tScheme is real, it's run by industry. So we said, 'Well, that worked in England, it's bound to work in America, surely.'"(G001, Interview)

Acceptance of External Credentials

To accept credentials generated outside the federal government, agencies needed to trust that they were appropriately bound to individuals. In the case of federal employees, agencies could trust the credential enrolment and issuance because it occurred under the auspices of the federal government itself, using established, secure processes. In the case of external identity providers, federal agencies had no oversight of their processes and therefore could not inherently trust the validity of a credential without a standardised method for judging it. This led the federal Office of Management and Budget (OMB) (2003) to promulgate memorandum M-04-04, a risk methodology for judging the "Level of Assurance" (LoA) that a credential was valid and appropriately bound to a single individual. The memorandum ordered all executive branch agencies to assess the degree and likelihood of harm that would result from loss of or unauthorised access to personal data in their possession. Agencies were to consider six categories of harm and impact in their assessment of risks from an authentication error:

> "• inconvenience, distress, or damage to standing or reputation
> • financial loss or agency liability
> • harm to agency programs or public interests
> • unauthorized release of sensitive information
> • personal safety
> • civil or criminal violations" (Office of Management and Budget [OMB], 2003, p. 5)

The potential impact values for these categories were Low, Moderate and High. OMB's risk methodology aligns the harm impact values with the Levels of Assurance of an asserted identity.

Figure. 5.1 Impact category/Level of Assurance matrix.

	Assurance Level Impact Profiles			
Potential Impact Categories for Authentication Errors	**1**	**2**	**3**	**4**
Inconvenience, distress or damage to standing or reputation	Low	Mod	Mod	High
Financial loss or agency liability	Low	Mod	Mod	High
Harm to agency programs or public interests	N/A	Low	Mod	High
Unauthorized release of sensitive information	N/A	Low	Mod	High
Personal Safety	N/A	N/A	Low	Mod High
Civil or criminal violations	N/A	Low	Mod	High

Source: OMB, 2003, p. 7

The Levels of Assurance are defined as follows:

> "Each assurance level describes the agency's degree of certainty that the user has presented an identifier (a credential in this context) that refers to his or her identity. In this context, assurance is defined as 1) the degree of confidence in the *vetting process* used to establish the identity of the individual to whom the credential was issued, and 2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued" (OMB, 2003, p. 4, orig. emphasis).

The levels are:

> "• Level 1: Little or no confidence in the asserted identity's validity
> • Level 2: Some confidence in the asserted identity's validity
> • Level 3: High confidence in the asserted identity's validity
> • Level 4: Very high confidence in the asserted identity's validity"
> (OMB, 2003, p. 5)

OMB's methodology standardised agencies' policies for judging confidence in external credentials. It allowed each agency to make its own determinations about the right mix of data sensitivity, potential harm, credential enrolment reliability and security model. One administrator stated:

> "Agencies were already trying to bring their services to the web, or to the internet, and for whatever reason were having trouble with that last

> mile, because the last mile's always the hardest. And so the idea was that we're going to put this together and actually help get them there. M-04-04 was a part of that.…" (G001, Interview)

Once an agency concluded its assessment, it was to select technology appropriate to the Level of Assurance as specified by the National Institute of Standards and Technology (NIST), a non-regulatory federal agency within the US Department of Commerce with a broad remit to advance measurement science, standards and technology. NIST's Special Publication 800-63 (Burr, et al., 2011) details security token types, token and credential management system types, authentication protocols, cryptography standards, and attack types to be defended against. As the consequences from an authentication error increase, so do the Levels of Assurance, as well as the required security strength of the identity management system.

Special Publication 800-63 also describes identity proofing requirements for credential issuers. Separated into 'in-person' and 'remote' applications for a credential, the publication specifies the types of existing identity proofs a person must provide to a credential issuer to validate his or her identity, the required method of validation, and any further actions the issuer must take to complete the identity assurance. For example, at Level of Assurance 3, in a remote application, an applicant must supply a government-issued ID number, such as a driver's license or passport number, and a financial or utility account number, such as a checking account number, a water bill account number, or a credit card number. The credential issuer verifies the applicant's identity "through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, [date of birth], address and other personal information in records are consistent with the application and sufficient to identify a unique individual" (Burr, et al., 2011, p. 34). Finally, the issuer confirms the applicant's address by sending information through the mail, or calls the applicant on the phone and "records the

[a]pplicant's voice or [uses] alternative means that establish an equivalent level of non-repudiation" (Burr, et al., 2011, p. 34).

Public-Private Authentication Initiatives

The policies to enable federal entities to accept non-federal credentials were grouped under the heading of the Electronic Authentication Initiative (EAI), under the management of the General Services Administration (GSA) (G003, Interview; G004, Interview; G006, Interview). US IDM policy-makers invited the Social Security Administration to consider becoming an authoritative source for citizen digital identities. They declined because the scale, complexity and the political unpalatability of building a system that could spark fears of national identification (G001, Interview). In 2004, a public-private partnership formed called the Electronic Authentication Partnership (EAP). This partnership represented industry players interested in commercially engaging the government on its authentication needs. The EAP aligned itself with Electronic Authentication Initiative policies and frameworks, including M-04-04 and Special Publication 800-63 (G003, Interview). To enter into business arrangements with potential vendors, the federal government attempted to create standardised agreements between it and all potential identity providers. The IDPs pushed back on the agreements, and federal officials were unable to administer a programme with variable bilateral agreements with a host of different vendors (G003, Interview; G008, Interview; Wilsher, Interview). Nor was the federal government in a position to certify all of the potential IDPs for compliance with relevant federal policy. An official explained:

> "… we really didn't want to have hundreds of bilateral agreements between the federal government and all these IDPs. So we were trying to get a standardised agreement, but if you're dealing with the financial services industry, you're dealing only with their legal department, and every one of them has got something, and so that's why [it] got top heavy.… And we couldn't be the entity to go out and do the

> assessments of everyone … we just couldn't reasonably set up [that] infrastructure." (G003, Interview).

Federal engagement with EAP failed, but the policy, commercial and intellectual work of it was merged with the Liberty Alliance, a standards development and management organisation focused broadly on identity federation and certification (G003, Interview). The merged organization renamed itself the Kantara Initiative ("Kantara"), and it remained closely involved in US identity management efforts.

Establishment of FICAM

In 2008, all US identity management policy and initiatives were put under the auspices of the Information Security and Identity Management Committee (ISIMC), a committee of the Federal CIO Council, itself made up of the Chief Information Officers (CIOs) of federal agencies and the defence and intelligence communities (G001, Interview). ISIMC formed the Identity, Credential and Access Management (ICAM) sub-committee whose remit included all management, security and privacy aspects of US identity management policy relating to interaction with and within the federal government (CIO Council, 2008).

With administrative support from the consulting firm Deloitte, FICAM (as ICAM came to be commonly known, inserting 'F' for Federal), released in 2009 its *Roadmap and Implementation Guidance* (Identity, Credential & Access Management [ICAM], 2009c). The Roadmap included requirements for FICAM to develop harmonised policies to allow federal agencies to accept externally-created credentials. One administrator recalled:

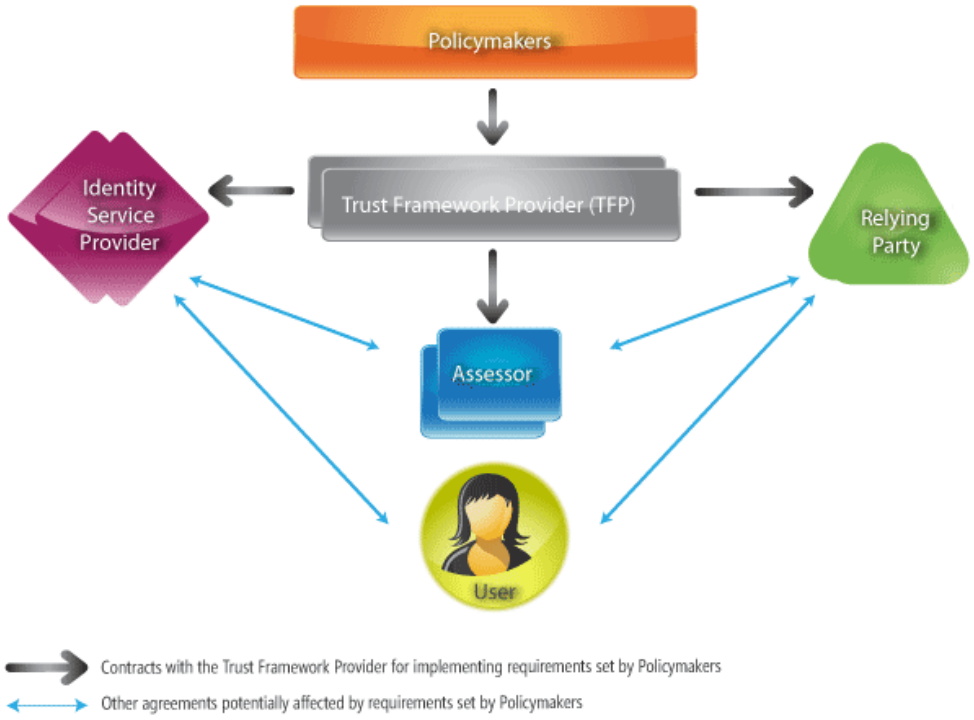
> "[W]e had workgroups that met regularly, which had representation from across the ICAM committee, which is the 25 major Federal CIO agencies.… Deloitte actually went out and interviewed people from the agencies on the different topics. Not just from the Federal agencies, but

> also from industry. So, there was an awful lot of collaboration and discussion that went into the writing." (G001, Interview).

Creation of Trust Frameworks

The failure of EAP led US policy-makers and administrators to advance a model informed by tScheme: the Trust Framework Provider model, or TFP (G008, Interview; N002, Interview; Don Thibeau [Thibeau], Interview; Wilsher, Interview). Rather than enter into bilateral agreements with would-be identity providers, FICAM envisioned a multi-party arrangement. A non-governmental entity would be placed between FICAM and vendors. It would be responsible for certifying the vendors against FICAM's requirements. FICAM would synthesise all of its requirements – operational, technical and privacy – into a single package; what it needed to 'trust' that vendors met the government's needs for identity services. The requirements package would be handed to a Trust Framework Provider, an intermediary who would publish those requirements and then certify participating entities against them. Those entities – for-profit companies, non-profits and universities – would provide identity credentials for use on government websites and resources. The Trust Framework Provider would accredit independent assessors to evaluate identity provider applicants and certify that their operational policies, technical architectures and privacy policies were comparable to those required by FICAM (ICAM, 2009d). The figure below illustrates the relationships of the Trust Framework model.

Figure 5.2 A Trust Framework



Source: Open Identity Exchange, 2013

FICAM's requirements contained the Level of Assurance risk methodology from the Office of Management and Budget's memorandum M-04-04 and NIST Special Publication 800-63's related technical, security and identity proofing requirements. A Trust Framework could thereby certify external credential providers against the Levels of Assurance. This way, potential identity providers could be certified to a specific Level, and agencies – relying parties (RPs) – could accept an IDP's credentials for services at that Level. FICAM codified how it would approve Trust Framework Providers in its Trust Framework Provider Adoption Process (TFPAP) (ICAM, 2009d). A government administrator explained:

> "[W]e couldn't be the entity to go out and do the assessments of everyone. … So what got built out of that in the next phase … was we developed the Trust Framework Provider Adoption Process, where we

> said … if we can work with entities that are operating under that same trust model, in other words policy compliance … and an assessment that they're following their policies and procedures … then, if we can assess those Trust Framework Providers and their rules and how they go about certifying, then it's a much more scalable model …" (G003, Interview)

Through this model, FICAM could amalgamate all federal requirements for the use of external credentials. This relieved federal agencies of many of the burdens connected to complying with the executive order to accept external credentials. Don Thibeau, Chairman of the Open Identity Exchange, an initial Trust Framework Provider, explained:

> "… if you think about Trust Frameworks, [they are] basically sets of specifications for interoperability. … the government would set out [specifications] that would also include a standard set of privacy requirements that had to be met in order for a commercial identity provider to be certified as per the … requirements that FICAM outlined. So, the opportunity was that … FICAM aggregated privacy requirements across multiple government agencies." (Thibeau, Interview)

Identity Scheme Adoption

The core of FICAM's citizen credentialing activities is the exchange of identity and attribute assertions between federal and non-federal entities. At a fundamental level, this means the passage of digital messages between the entities; putting 'bits on the wire.' Disparate entities operate a variety of heterogeneous IT equipment and software. For two or more entities to interoperate with each other's IT systems, they must agree upon the method of interoperation. This is the domain of standards and protocols, which define ways for technical systems to interoperate with one another. For FICAM to harmonise the elements necessary for government relying parties to accept credentials from a set of as-yet unknown identity providers it needed to stipulate technical interoperability specifications – how to send and interpret the bits on the wire – for each party to communicate.

A number of federated identity management standards existed. The standards could be configured in a variety of ways; they were supersets of all possible features. To meet its technical, security and privacy requirements, FICAM needed to constrain the standards' features. FICAM termed the constrained subsets "schemes" and created a formal Identity Scheme Adoption Process (ICAM, 2009a). Three identity standards were selected to go through the Scheme Adoption Process: OpenID 2.0, Secure Assertion Markup Language 2.0 (SAML), and Identity Metasystem Interoperability 1.0 (IMI). FICAM's Architecture Working Group evaluated each standard for its suitability in government federation efforts. This included selecting the subset of features and configuration that would meet FICAM's requirements. One government administrator recalled:

> "So FICAM says well let's build the policies for how we can adopt technologies, standards and protocols in the federal government and how we go about doing that. So we called that mix of technologies, protocols and standards, 'schemes'… And so we wrote a policy document … called… the Scheme Adoption Process.… And so, that document [says] in order to adopt the scheme, they'll have to be industry-based consensus standards in place, standards have to be around long enough to mature to the point where there [are] sufficient products implementing those standards…" (G003, Interview)

Pseudonymous Identifiers

Each of the three schemes adopted by FICAM was configured to allow the option for relying parties to request a pseudonymous identifier. With regard to the citizen credentialing component of US identity management policy, the scheme configuration is currently the most concrete technical requirement for unlinkability. In theory, a citizen could use a digital identity credential from a FICAM-approved provider to access a federal resource. The hosting agency could request the provider to send a pseudonym in lieu of personally identifying information (PII) about the citizen. However, Level of Assurance 3

and 4 require a meaningful name to be transmitted as part of an identity assertion. Ergo, unlinkability is only possible in Level of Assurance 1 and 2 transactions (Burr, et al., 2011).

The identity scheme configurations pre-date FICAM, originating in the Electronic Authentication Partnership (G008, Interview; P006, Interview). The same consultants, Chris Louden and Dave Silver, were involved in the technical efforts of both EAP and FICAM, and FICAM inherited many of the configurations created for EAP (P006, Interview). This included the requirement for an ability to use pseudonymous identifiers. The impetus for the requirement was the consultants' informal support of the principle of data minimisation (P006, Interview). One recent definition of data minimisation in US policy is:

> "Organizations should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s)" (White House, 2011, p. 45).

This principle is part of what are commonly referred to as the Fair Information Practice Principles, or FIPPs, seen as influential on US informational privacy policies (explained further below) (G001, Interview; G003, Interview; G006, Interview; N005, Interview; Gellman, 2012). The relationship between unlinkability and data minimisation is discussed in the "Relationship to minimisation" section below.

Privacy Criteria

In addition to the limited privacy considerations codified in the adopted schemes, the Trust Framework Adoption Process (ICAM, 2009c) contained privacy requirements for prospective identity providers. The criteria were:

> "Opt-in: IDPs must obtain positive confirmation from an end user before transmitting any information to any government applications.

> Minimalism: IDP must only transmit attribute information that was explicitly requested by an RP.
>
> Activity Tracking: IDPs must not disclose information on end user activities with anyone and must not use the information for any purpose other than the federated identity service.
>
> Adequate Notice: IDPs must provide adequate notice of the nature of authentication events, any transactions with the RP, the purpose of the transactions, and a description of any disclosure or transmission of PII to any party.
>
> Non-Compulsory: Agencies should provide alternative forms of access so that a 3rd party identity service is not required to access federal resources.
>
> Termination: In the event that and IDP terminates its federated identity service, it shall continue to protect any PII it holds." (ICAM, 2009c, p. 12)

It should be noted that the above definition of 'Minimalism' is not a full evocation of the data minimisation principle contained in the FIPPs and related privacy frameworks. In the TFPAP definition, the 'burden' of minimising the data falls exclusively on federal agencies. However, the recommendation and requirement for pseudonymous identifiers in the identity schemes shifts some of the burden back to the identity providers.

The privacy criteria were authored by members of the Identity Management Subcommittee of the Privacy Subcommittee of the CIO Council. Two administrators recalled:

> "… when we established the ICAM Subcommittee, a few folks from the Privacy Subcommittee came to us and said, "Privacy: bake it in, don't bolt it on." … And, so Naomi Lefkovitz … and Debra Diener … They established an identity management subcommittee under the Privacy committee with Debbie and Naomi leading it … So the privacy language in the ICAM roadmap was drafted by them." (G001, Interview)

> "There is an interagency Privacy Council which are privacy leads for different federal agencies … tying that group into FICAM was really that bridge.… So the work that … spearheaded applying FIPPs to FICAM requirements originated out of that group … I think that they relished the opportunity that they were being brought into the FICAM picture and were able to work on policies that would be implemented … They responded very strongly to being included in the FICAM development and initiative…." (G003, Interview)

The privacy criteria were added near the end of the FICAM development process, and largely focused on restricting the behaviour of identity providers, not government relying parties (G004, Interview; G006, Interview; N003, Interview). At the time of this writing, privacy guidance for government agencies is still in an unpublished, draft form (G009, Interview). The privacy criteria became part of the assessment performed against identity providers in order to become a FICAM-approved credential provider. An administrator explained:

> "… FICAM went one step further and said, 'Well, we also have these privacy principles that we want applied to any IDP,' and it's up to the Trust Framework provider to build the infrastructure for how that assessment is performed for identity providers: the policy … procedural … and the operational compliance of any provider, and to do that certification of providers." (G003, Interview)

FIPPs in FICAM

The FICAM privacy criteria are largely informed by and derived from the Fair Information Practice Principles (G001, Interview; G003, Interview; G006, Interview; Greenwood, Interview). The eight principles of the FIPPs are:

> "• Transparency: Organizations should be transparent and notify individuals regarding collection, use, dissemination, and maintenance of personally identifiable information (PII).
>
> • Individual Participation: Organizations should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII.

> Organizations should also provide mechanisms for appropriate access, correction, and redress regarding use of PII.
>
> • Purpose Specification: Organizations should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.
>
> • Data Minimization: Organizations should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).
>
> • Use Limitation: Organizations should use PII solely for the purpose(s) specified in the notice. Sharing PII should be for a purpose compatible with the purpose for which the PII was collected.
>
> • Data Quality and Integrity: Organizations should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.
>
> • Security: Organizations should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
>
> • Accountability and Auditing: Organizations should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements." (White House, 2011, p. 45)

From the above principles, "Transparency" and "Purpose Specification" inform FICAM's "Adequate Notice" provision (see pp. 125-126). "Individual Participation" informs the requirement for "Opt-In." "Data Minimization" informs FICAM's "Minimalism" requirement and is supported by the pseudonymity features of the identity schemes. "Security" informs the "Termination" provision, and "Accountability and Auditing" supports the requirement for on-going audits of identity providers specified by the Trust Framework Provider Adoption Process (ICAM, 2009d, pp. 12-13)

The FIPPs themselves have evolved since the early 1970s (Gellman, 2012). Beginning with the US Department of Health, Education and Welfare's (1973) report, *Records, Computers and the Rights of Citizens*, the core principles of the FIPPs have appeared in a variety of US and European laws and policy instruments, including the Privacy Act of 1974, the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980), and the European Data Protection Directive (1995) (Gellman, 2012, pp. 2-7). Some respondents viewed FICAM's application of the FIPPs as a positive, evolutionary step in US privacy policy (G003, Interview; Greenwood, Interview). One administrator opined:

> "So what FICAM did was bold in saying … 'these are the rules, these are the privacy rules that we are going to apply to this online environment with the federal government as relying party….' They didn't base it on the Privacy Act, they didn't try to extend the Privacy Act … to non-federal entities or non-federal information systems. What they said was, 'This is how you are going to do business with us and these are our rules and it is important.'" (G003, Interview)

Dazza Greenwood, an MIT lecturer and legal expert on identity management, observed:

> "The fact that there are some fair information practices in FICAM assessment criteria at all is a major step forward toward fair information practices in the United States and it's good." (Greenwood, Interview)

Cybersecurity Policy Review

As FICAM was developing its policies, the White House (2009, p. iii) released a Cyberspace Policy Review, a "comprehensive, 'clean-slate' review to assess U.S. policies and structures for cybersecurity" ordered by President Barack Obama in the early part of his presidency. This Review highlighted identity management as critical to the development of comprehensive national cybersecurity while also focusing on privacy:

> "We cannot improve cybersecurity without improving authentication.… Identity management also has the potential to enhance privacy through additional protection against the inappropriate release of personally identifiable information." (White House, 2009, p. 33)

One administrator described the realisation in government of the importance of identity management:

> "So what happened in 2009 or so there was this realisation that as a government we weren't paying as much attention to identity management as we should be and it was becoming the new important thing when it comes to information security." (G001, Interview)

The FICAM Roadmap (ICAM, 2009c, p. 1) cites the Cyberspace Policy Review as a specific policy influence:

> "Identity, Credential, and Access Management (ICAM) efforts within the Federal Government are a key enabler for addressing the nation's cybersecurity need. The Cyberspace Policy Review includes an entire section on the use of identity management in addressing cyber threats. The report includes a near-term action to develop 'a cybersecurity-based identity management vision and strategy that addresses privacy and civil liberties interests, leveraging privacy-enhancing technologies for the Nation.'"

OpenID and the Open Identity Exchange

The Chief Information Officer of the US government, a member of the Obama Administration (2008–2016), informed the FICAM administrators that OpenID, a federated identity standard, should be a priority (G003, Interview; Scott David [David], Interview; Thibeau, Interview). It was deemed valuable because of its ostensible ubiquity (G003, Interview). OpenID went through the Scheme Adoption Process and it was determined that the standard would need to be altered to accommodate the government's requirements (N003, Interview). Ultimately, the OpenID 2.0 specification became able to be adopted by FICAM. A government administrator recalled:

> "Our Chief Information Officer came to us at GSA and said … 'millions of people have these OpenIDs. Figure out how the federal

> government can accept them.' So [for] the Scheme Adoption Process … we would usually look to demand from the federal government agencies for [a] particular technology or protocol. In this case, the CIO of the government said, 'Figure out how to use OpenIDs.' So, we looked at the Scheme Adoption Process, applied that, adopted the OpenID specification and how it would be implemented." (G003, Interview)

To embrace OpenID technology, the CIO of the US Government approached the Open Identity Foundation (OIDF), the organization responsible for managing the OpenID standard (G003, Interview; David, Interview; Thibeau, Interview). The OIDF is largely comprised of industry players who have a stake in the commercial dimension of the OpenID standard. Don Thibeau recalled:

> "[T]he government sought out the OpenID Foundation because they saw it frankly as two things. One: a singular place where they could talk to many companies; companies like Microsoft in the enterprise space, Google in search, Facebook in social, Symantec and others in security. So, from the government's point of view, they looked for an efficient way to talk to industry. And … from a process point of view, it is easier for them to engage non-profit organisations – standards-oriented organisations – than it is for-profit." (Thibeau, Interview)

There was disagreement among members as to whether to engage with the federal government, so a new organization was spawned specifically to meet the government's needs: the Open Identity Exchange (OIX) (David, Interview; Thibeau, Interview). Don Thibeau explained:

> "… the reaction from the Open Identity Foundation was mixed. Some companies saw that engagement as an inevitable or necessary or positive one and others wanted to take a much more passive role. So essentially the OIX was created in part with a grant from the OpenID Foundation but also funding from companies like Google, AT&T, Verizon and others… So some of the member companies … saw this … engagement with the government as a necessary function of their footprint in the industry, and other companies … did not see that this was the time or the manner that they wanted to engage the government in these kinds of issues. So the OIX was created and some companies joined and other companies have not." (Thibeau, Interview)

OIX became the testing ground for the Trust Framework Provider model. As a provisionally-accepted TFP, OIX oversaw the certification of five companies: Google, Equifax, PayPal, VeriSign and Wave Systems (IDManagement.gov, n.d. a). OIX engaged a professional in the IT auditing community, John Steenson, to be the initial Assessor to certify that the companies' operational, technical and privacy policies were comparable to FICAM's requirements (Thibeau, Interview).

Three other Trust Framework Providers were ultimately approved: the Kantara Initiative, the entity born of the merger of the Electronic Authentication Partnership and the Liberty Alliance; InCommon, a federation operator focused on higher education and research institutions and relevant commercial actors; and SAFE-BioPharma, an industry association of medical and pharmaceutical organisations and supporting companies (IDManagement.gov, n.d. b).

National Strategy for Trusted Identities in Cyberspace

In April of 2011, the White House (2011, p. i) released the National Strategy for Trusted Identities in Cyberspace (NSTIC), "a strategy to make online transactions more secure for businesses and consumers alike." The NSTIC envisioned an 'identity ecosystem' comprised of all parties who have a stake in trustworthy online interactions – individuals, organizations and governments "…where individuals and organizations will be able to trust each other because they follow agreed upon standards to obtain and authenticate their digital identities.…" (White House, 2011, p. 2). The NSTIC is an "aspirational policy" (G007, Interview) that serves as a rallying point for US identity management efforts, though does not carry the force of legislation. It is 'soft law' – the US is encouraging it as a national strategy but it is neither a formal compliance regime nor does it carry sanctions. It emphasises that US national identity management efforts are to be industry-led, digital identities are to be

voluntary and not a form of national ID, and that identity solutions are to be privacy-enhancing.

The NSTIC states clearly that private industry should lead the efforts to create more trustworthy online credentials for the citizenry:

> "The private sector will lead the development and implementation of this Identity Ecosystem, and it will own and operate the vast majority of the services within it. The Identity Ecosystem should be market-driven, and it should provide a foundation for the development of new and innovative services." (White House, 2011, p. 4)

> "The role of the Federal Government is to support and enable the private sector …" (White House, 2011, p. 4)

> "… the Identity Ecosystem will emphasize non-proprietary, international, and industry-led standards." (White House, 2011, p. 14)

This emphasis relates to the government's awareness of the strong antipathy towards national identification, explored in the National ID theme section below. The private character of US citizen credentials is a key difference with German policy; this is explored in Chapter 7. Relatedly, the NSTIC explicitly states that it is not part of plan to create a national ID:

> "… the Strategy does not advocate for the establishment of a national identification card or system …" (White House, 2011, p. 8)

It further states that participation in the proposed identity ecosystem will be voluntary:

> "… participation in the Identity Ecosystem will be voluntary: the government will neither mandate that individuals obtain an Identity Ecosystem credential nor that companies require Identity Ecosystem credentials from consumers as the only means to interact with them." (White House, 2011, p. 12)

This clear language illustrates the government's perceived need to allay Americans' fear that NSTIC credentials would be used as part of a national identification effort.

The NSTIC states that identity solutions are to be privacy-enhancing:

> "The enhancement of privacy and support of civil liberties is a guiding principle of the envisioned Identity Ecosystem." (White House, 2011, p. 2)

> "The role of the Federal Government is to … enhance the protection of individuals; and ensure the guiding principles of privacy …" (White House, 2011, p. 4)

Notably, the NSTIC specifically identifies pseudonymity and anonymity as key goals:

> "It is vital to maintain the capacity for anonymity and pseudonymity in Internet transactions in order to enhance individuals' privacy and otherwise support civil liberties." (White House, 2011, p. 1)

> "In addition to privacy protections, the Identity Ecosystem will preserve online anonymity and pseudonymity, including anonymous browsing." (White House, 2011, p. 2)

> "Nor does the Strategy seek to circumscribe the ability of individuals to communicate anonymously or pseudonymously, which is vital to protect free speech and freedom of association." (White House, 2011, p. 8)

This language is a significant public commitment to modern privacy principles. Furthermore, the NSTIC details unlinkability goals without naming them as such:

> "The Identity Ecosystem will use privacy-enhancing technology and policies to inhibit the ability of service providers to link an individual's transactions, thus ensuring that no one service provider can gain a complete picture of an individual's life in cyberspace." (White House, 2011, p. 2).

> "The offline world has structural barriers that preserve individual privacy by limiting information collection, use, and disclosure to a specific context. For example, consider a driver's license: an individual can use a driver's license to open a bank account, board an airplane, or view an age-restricted movie at the cinema, but the Department of Motor Vehicles does not know every place that accepts driver's licenses as identification. It is also difficult for the bank, the airport, and the movie theater to collaborate and link the transactions together." (White House, 2011, p. 11)

> "The Identity Ecosystem will… protect individuals from those who would link individuals' transactions in order to track individuals' online activities." (White House, 2011, p. 17)

> "[Strong privacy] protections will ensure that the default behaviour of Identity Ecosystem providers is to: … Minimize data aggregation and linkages across transactions …" (White House, 2011, p. 30)

This type of language occurs in very limited amounts in other US policy documents (Federal Trade Commission, 2012; White House, 2012). Partly, this is because the NSTIC is a more of a call to action than an implementable policy initiative. But, in contrast to existing US law and data protection frameworks, it is ambitious language that has the potential to inform the character of future policy. This is certainly the case in the design of the Federal Cloud Credential Exchange, detailed below.

The NSTIC highlights the role of standards in its privacy protection goals:

> "... privacy-enhancing technical standards ... will minimize the transmission of unnecessary information and eliminate the superfluous 'leakage' of information that can be invisibly collected by third parties. Such standards will also minimize the ability to link credential use among multiple service providers, thereby preventing them from developing a complete picture of an individual's activities online." (White House, 2011, p. 12)

This is evidence of the technocratic nature of identity management policy, and it points out the need for multi-stakeholder governance. The above quote illustrates policy that intersects the norms and values of governments and

standards developers. It also shows the critical role of technical standards in identity management. This is evident in the German case as well. German unlinkability relies on established standards for cryptography and secure internet communications. When the German government determined that the basis for exchanging passwords across a contactless card interface was insecure, it created a new, more secure standard that was ultimately adopted by an international standards body. See Chapter 6 for a complete explanation.

The NSTIC grounds its privacy rationale in the Fair Information Practice Principles:

> "The Fair Information Practice Principles (FIPPs) are the widely accepted framework for evaluating and mitigating privacy impacts… The envisioned Identity Ecosystem will be grounded in a holistic implementation of the FIPPs in order to provide multi-faceted privacy protections." (White House, 2011, pp. 11-12)

> "… a FIPPs-based approach will promote the creation and adoption of privacy-enhancing technical standards …" (White House, 2011, p. 12)

> "… implementation of the FIPPs will protect individuals' capacity to engage anonymously in cyberspace. Universal adoption of the FIPPs in the envisioned Identity Ecosystem will enable a variety of transactions, including anonymous, anonymous with validated attributes, pseudonymous, and uniquely identified – while providing robust privacy protections that promote usability and trust." (White House, 2011, p.12)

The NSTIC authors needed to use the non-binding FIPPs as a basis because of the lack of other applicable frameworks (such as an omnibus personal data protection law) to draw upon. As with FICAM, some respondents saw NSTIC's use of and reliance on the Fair Information Practice Principles as an important step in the advancement of privacy goals in the United States (G003, Interview; Greenwood, Interview; N005, Interview). Dazza Greenwood observed:

> "For the first time ever at the highest level of government with a lot of agency integrated effort behind it and a lot of private sector cheerleading around it, we have a couldn't-be-more-clear statement that FIPPs needs to apply across the whole society and every sector of the economy.… That's notable to me." (Greenwood, Interview)

NSTIC has been described as 'FICAM for the commercial domain' (G001, Interview; G007, Interview; N002, Interview), and it clearly draws upon FICAM's earlier policy development. A government administrator noted:

> "FICAM is how the government is taking caring of its own space; the government is a first or second party to a transaction. So if you think of somebody… there's a lake and somebody drops something in the middle of the water … that's FICAM. And as the ripples go out, that's NSTIC. So we take the work that we did in FICAM and we're applying it, we're saying, 'Can we create that same kind of trusted environment that we're creating for ourselves for the rest of the country?' And so the work we've done in FICAM is informing the work that we're doing in NSTIC." (G001, Interview)

Accordingly, the NSTIC declares an intention to integrate FICAM's policy development:

> "The Federal Government is already seeking to create this world for its own operations by executing the Federal Identity, Credential, and Access Management (FICAM) Roadmap. The Strategy seeks to accelerate those activities and to foster the development of an Identity Ecosystem in which trusted identities are available to any individual or organization." (White House, 2011, p. 6).

> "Building upon FICAM, all online Federal Executive Branch services are aligned appropriately with the Identity Ecosystem and, where appropriate, accept identities and credentials from at least one of the trustmarked private-sector identity providers." (White House, 2011, p. 41)

Relatedly, an administrator remarked that the policy influence between FICAM and NSTIC goes both ways:

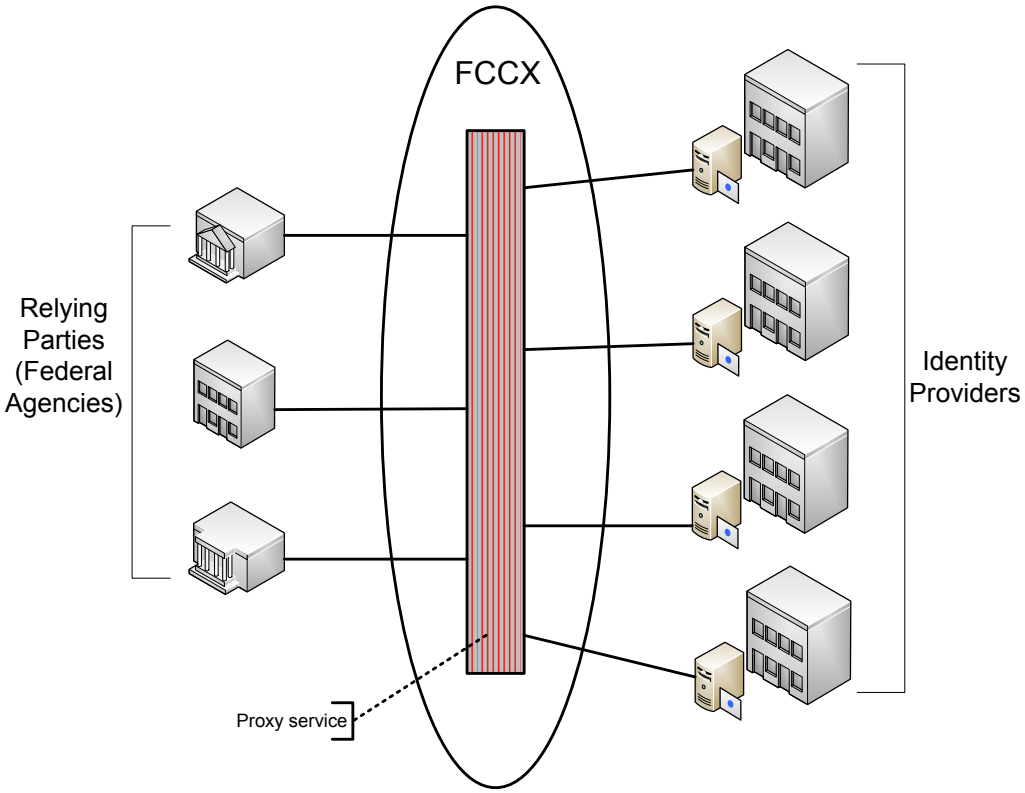
> "… if by some chance the NSTIC comes across … something new and wonderful that FICAM didn't think of, we'll go back in and FICAM will get adjusted." (G001, Interview)

National identity management policy includes credentialing activities for e-government and commercial use. The thesis finds that e-government, the delivery of public services and citizen digital identities are intrinsically tied together. However, digital identity is multi-faceted, and the separation between public uses of citizen credentials and private/commercial uses of them is an artificial one. This is well illustrated by the US Personal Identification Verification (PIV) initiative to create reliable credentials for physical and logical access by federal employees and contractors. PIV cards are issued by the federal government, but PIV-interoperable (PIV-I) cards, based on identical technical and operation rules, provide access to both federal resources and to private ones (Smart Card Alliance, 2012). National identity management policies and standards influence and are influenced by private endeavour. The definition of identity management policy, proposed in Chapters 4 and 7, accounts for this public/private relationship.

Federal Cloud Credential Exchange

Building, configuring and maintaining the technology necessary to accept identity assertions is non-trivial. In early 2012, federal administrators and policy-makers realized they needed additional infrastructure to enable agencies to accept externally-created credentials. Federal relying parties were not positioned to accept credentials despite ten years of various IDM initiatives. The one exception to this was the National Institutes of Health, who built a federated identity system called iTrust in 2009 (G004, Interview). To harmonise efforts and achieve economies of scale, government officials decided to procure technical infrastructure that could be centrally controlled and made available to all agencies. The infrastructure was dubbed the Federal Cloud Credential Exchange, illustrated below.

Figure 5.3 Proposed Federal Cloud Credential Exchange



This proposed infrastructure would minimise start-up and maintenance costs for agencies, and accelerate policy implementation. Further, the FCCX would offer an additional technical layer to enforce privacy policies. The FCCX would sit between identity providers and relying parties, in theory providing the ability to blind identity providers and relying parties from one another. One senior official noted that the FCCX is a government-wide implementation of the NIH iTrust service (G004, Interview).

A stated goal of the Federal Cloud Credential Exchange is "[p]reserving privacy (minimize storage of personal information and 'panopticality' of the service)" (Gallagher and Lefkovitz, 2012). Panopticality is a reference to the "panopticon," an 18th century prison design by Jeremy Bentham (1995) that

allows all prison cells to be seen into while preventing prisoners from knowing when they are being watched. It is a common trope in privacy discourse, emphasizing the invisible, pervasive monitoring possible in electronic systems (Gandy, 1993; Lyon, 2003; Reiman, 1995; Uteck, 2009). Explaining its application here, FICAM and NSTIC officials write that panopticality is:

> " 1. It is the ability of Credential Providers to 'see' all the Service Providers to which a citizen authenticates
>
> 2. It is the visibility that the FCCX service itself may have into the citizen information that is flowing thru [*sic*] it" (Gallagher and Lefkovitz, 2012)

The evolving, proposed architecture for the FCCX enables a degree of unlinkability that prior architectures, relying solely on the inherent privacy characteristics of SAML and OpenID, were unable to achieve. Those two protocols were able to provide a pseudonym for each user on a per-relying party basis – each relying party would see a different pseudonym for the same user. Without other identifying information (such as an email address), this would prevent one relying party from knowing that the user was visiting another relying party. However, the identity provider would know everywhere the user used her credential. The FCCX has the potential to not only blind relying parties from one another, but also blind the identity provider from the particular uses of its credential. A citizen could use a trusted credential at multiple relying parties, but each relying party would be ignorant as to which other relying parties the citizen visited. And, the identity provider would be ignorant to all of the relying parties she visited. Also, the FCCX 'layer' itself would, in theory, also not retain information about a user's activity (G009, Interview).

At the time of this writing, the FCCX is still in a design phase. If implemented in the manner described above, it would be the US's most comprehensive set

of policy and technical requirements for unlinkability. In August 2013, SecureKey, a Toronto-based identity management and security company, was awarded a contract to build and manage a one-year pilot of the FCCX (SecureKey, 2013). SecureKey was previously involved in national identity management initiatives in Canada.

Policy summary

To summarise, as of September 2013, the privacy goal of unlinkability is emerging within US identity management policy aimed at citizens. Identity providers using FICAM's approved configuration of the OpenID protocol are required to use a pseudonym for each relying party that a user visits, and it is a recommended practice for SAML-based credentials. This is true, though, only for transactions at Level of Assurance 1 and 2. The proposed FCCX will also technically enforce unlinkability, but is still being designed, and so details are not yet available. With regards to non-technical enforcement, FICAM's Activity Tracking requirement prevents identity providers from using and sharing information they learn in the course of providing credentials to users. Practically, this means they may not link information about a citizen's e-government usage with anything else they know about her, or share that information with business partners. As to the National Strategy for Trusted Identities in Cyberspace, pilot projects are only just being funded to explore a range of topics. The strong unlinkability language it espouses is as yet a strategic goal; an aspiration of the various stakeholders and authors that contributed to it. In September 2012, the National Institute for Standards and Technology announced an award of $9 million to five US organisations to create pilot projects to explore the NSTIC's goals of privacy-preserving, secure online transactions.

Themes

The remainder of the chapter is dedicated to exploring various themes that emerged from the data in order gain a holistic picture of the origins and future of US unlinkability. The themes were generated through analysis of the empirical data and a review of primary and secondary sources. Given the paucity of academic research of US citizen credentialing generally and unlinkability specifically, most of the themes were discovered inductively (Braun and Clarke, 2006) and through review of literature on broader identity management subjects. See the *Analysis* sub-heading in Chapter 3 for a complete explanation of the thematic analysis techniques employed. The headings of the sections are derived from the thematic coding and analysis of the data.

The first part of this section explores the influence of the American rejection of national identification systems. In relation to the thematic categories generated during analysis of the empirical data, national identification was a major issue that emerged from the Cultural category. Following this, various policy and technical dimensions of unlinkability are analysed, including data minimisation, enforcement, and the translation of the physical world into the electronic. These emerged from the analytic categories of Policy and Architecture & Standards. The next section details how US identity management policies are intrinsically tied to commercial interests and standards. This emerged from the Business analytic category. An analysis of policy compliance versus policy comparability follows, and the chapter concludes with a discussion of the role of consultants and the criticality of usability issues. These arose from the Policy, Players, and Usability categories, respectively.

National ID

A pervasive theme within this case is the spectre of a national identification system. Or rather, the acknowledged political impossibility of proposing a policy instrument that "smacks of a national ID" (G001, Interview). When discussed by respondents, it was taken for granted that any proposed system bearing a resemblance to a national identification initiative would suffer a withering attack by privacy advocates, the citizenry and government officials alike, with no chance of coming to fruition. One administrator explained:

> "… whenever you talked about a centralised organisation managing identities in the federal government, you come to national ID card, even if it's a virtual national ID card. You still end up there – somebody will raise that, and then everything dies when that happens, everything stops." (G001, Interview)

National identification, it is feared, could lead to greater government profiling of citizens (G001, Interview; N005, Interview; N006, Interview). This constraint foreclosed the government's ability to create an authentication infrastructure that would be directly managed by the government itself. This was true even if such a programme was limited only to interaction with government websites (G001, Interview). The national ID constraint is the strongest reason that the US government chose to rely on credentials created externally, which in turn triggered the need to create policy instruments to allow government agencies to judge the validity and authenticity of those credentials. In countries with national identity infrastructures that lent themselves to online authentication of citizens, such as Germany, this need did not exist (see Chapter 6). Identity assertions rooted in official national identity schemes could be inherently trusted by agencies since the underlying processes that created those digital identities were administered by their respective governments. As such, these other countries did not create policy instruments akin to the Level of Assurance methodology relied upon by the United States.

Relationship to minimisation

If there is a privacy/data protection policy antecedent to unlinkability, it is the principle of data minimisation. This principle has been formulated and restated in a number of US policies and reports, as well as those of the Organisation for Economic Coordination and Development, the European Union and other nations (Gellman, 2012, pp. 6-7). In 1977, a US presidential committee on informational privacy articulated eight principles that it believed were part of the US Congress's intent when it passed the landmark Privacy Act of 1974 (Privacy Protection Study Commission [PPSC], 1977, Chapter 13). It dubbed one of those principles, "The Collection Limitation Principle": "There shall be limits on the types of information an organization may collect about an individual, as well as certain requirements with respect to the manner in which it collects such information" (PPSC, 1977, chapter 13; Gellman, 2012, p. 4). In the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, the Collection Limitation Principle is restated as "There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject" (Gellman, 2012, p. 6; OECD, 1980, Part Two). The NSTIC recasts this principle under the heading Data Minimization:

> "Organizations should only collect [personally identifiable information] that is directly relevant and necessary to accomplish the specified purpose(s) and only retain [personally identifiable information] for as long as is necessary to fulfill the specified purpose(s)" (White House, 2011, p. 45).

Seen through this lens, unlinkability is an attempt to minimise the amount of information collected and shared about a person's online activity. This principle was cited by some as a justification for the inclusion of pseudonymity requirements and/or unlinkability goals (G006, Interview; P005, Interview) It places unlinkability in the broader context of the global evolution of privacy

principles; as an application of prior privacy goals to the changing technical landscape of an electronic society. The data minimisation principle is also international in scope, which partly explains the appearance of unlinkability policy goals in countries such as Canada, the UK, Germany, and Austria.

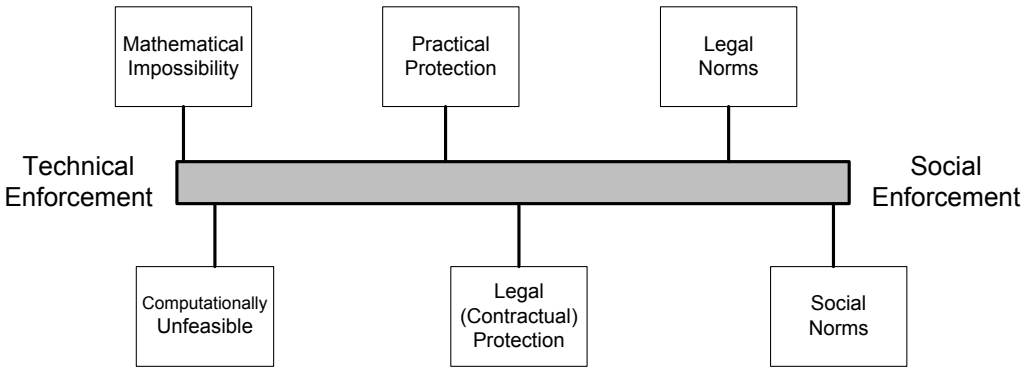
Spectrum of enforcement

Unlinkability is a not a uniform state; it is a multi-dimensional technical and policy strategy. It is best viewed, with regard to policy, as a spectrum. Drummond Reed, a former Executive Director of the Open Identity Exchange and the Information Card Foundation, a standards development organisation, conceptualises unlinkability as a 'level of blindness':

> "Blindness is probably a good metaphor because… my great-great aunt was legally blind, and she could still see enough to do a few things." (Drummond Reed [Reed], Interview)

Reed's views on unlinkability can be expressed in the following diagram:

Figure 5.4 Reed's spectrum of unlinkability



One side of the spectrum, the highest degree of unlinkability, is mathematical impossibility, where a credentialing system employs cryptography thought to be mathematically unbreakable. Next is the computationally unfeasible, employing cryptography that, while not mathematically impregnable, would be

unfeasible to break given the state of modern computing. "And those two are so close," Reed notes, "[that] I don't spend a lot of time distinguishing between them, because the technologies [that] are able to achieve either one are relatively few…." (Reed, Interview). The next point on the spectrum is "legal or practical protection" (Reed, Interview), where a system is configured in a privacy-preserving way but without the use of cryptography. For example, an identity provider can send a different pseudonym to each relying party, blinding the relying parties to the user's other activity. In this case, the identity provider knows where the user is going, but because of legal or contractual reasons would restrict disseminating the information; the relying parties would be denied the information by design. The final points on the spectrum are legal norms and social norms – external forces that are not enshrined in a system design, but exert a pressure nonetheless to constrain the release of information about a person's online activity. These could be contracts, laws, or cultural barriers. The spectrum of unlinkability is also a spectrum of enforcement, from a reliance on the technical to reliance on social forces.

Reed's spectrum is a valuable tool in evaluating policy choices. In service of improving policy-making, explicating the 'levels' of unlinkability provides a greater array of responses to the policy problem of protecting privacy in the digital identity space. Analytically, it allows for Germany and the US to be compared in way that preserves the particular methods each country's policy-makers pursued. This reflects the interdisciplinary nature of identity management research, marrying computer science with policy analysis.

Relationship to Activity Tracking

The privacy requirements section of the Trust Framework Provider Adoption Process includes a ban on "Activity Tracking":

> "Commercial Identity Provider must not disclose information on End User activities with the government to any party, or use the information

> for any purpose other than federated authentication" (ICAM, 2009d, p. 12)

In line with Reed's spectrum of unlinkability, this requirement can be seen as a legal/practical constraint on the release of information pertaining to a user's online activity. Since an identity provider will know everywhere a user logs in, this restriction by FICAM creates a form of unlinkability by preventing the identity provider from sharing knowledge of a user's online activity. It is a legal/practical constraint because the identity provider is limited by FICAM's requirements as promulgated by the managing Trust Framework.

Translating the physical world to the electronic

Part of the intention behind a policy of unlinkability is to recreate social conditions in the physical world. There is a perennial reference to the privacy characteristics inherent in a driver's license:

> "The offline world has structural barriers that preserve individual privacy by limiting information collection, use, and disclosure to a specific context. For example, consider a driver's license: an individual can use a driver's license to open a bank account, board an airplane, or view an age-restricted movie at the cinema, but the Department of Motor Vehicles does not know every place that accepts driver's licenses as identification. It is also difficult for the bank, the airport, and the movie theatre to collaborate and link the transactions together." (White House, 2011, p. 11)

The same unlinkable arrangement is evident with the use of cash. Though cash 'asserts' a monetary value rather than identity attributes, the effect is the same. A government's mint (the identity provider) releases cash (a credential) that can be trusted and used by merchants (relying parties) without being able to link the cash to the person or to the other uses the cash has been subject to. Andrew Nash, Google's former head of identity management, was involved in the development of the identity federation technology, SAML. He noted that mimicking the unlinkable qualities of cash was an intentional goal:

> "… in the Liberty Alliance when we actually defined [unlinkability] for SAML usage models, we were trying to protect the privacy of the users so that we could keep some level of anonymity as an analogue to a cash-based society… [that] was kind of the motivation. And it you know it makes sense. There's a whole a bunch of things you could do without you actually giving away who you are." (Andrew Nash [Nash], Interview)

Another subject viewed the analogies to cash and the driver's license as a design ethos within the technical communities of identity management:

> "It's just a beautiful thing, right? It's like cash and the driver's licence… you take it for granted, it's such a beautiful thing. And we are so far from doing that online… I think the techies and a lot of the [identity technology community], we just can't help it. We get up in the morning and we think about distributed systems, we think about anti-centralisation whatever, we try to shift control out to the edge of networks and we all feel, I think we all have this natural feeling like shouldn't we be sovereign actors, and shouldn't information about us be sort of as much as possible under our fingertips and controls?... [I]t's just a natural response to say, 'Well, why we don't build systems like that?' And the real world works that way. When you pull your wallet out with *your* cards, and it's a very private, secret thing, what's in your wallet … it just seems so natural to try and build a system that way." (Paul Trevithick [Trevithick], Interview)

However, another respondent also involved in standards development saw the driver's license example as misleading because it assumes that no other information is passing to the liquor store.

> "Assuming that you actually make a purchase, you give the merchant your credit card number which them gives them an omni-directional identifier and they can find out what last twelve things you've purchased you know, where you live… so you know it's a nice theory… [A]s long as you allow linkability through other mechanisms, you know sometimes you are just bending yourself out of shape for no good reason." (N003, Interview)

Commercial influences

The quote above introduces the most important theme that emerges from the US case data: the inseparability of commercial considerations from policy

intentions. Two essential sub-themes are consistently present in the empirical data: the need for personal data in normal business operations, and private businesses' need to earn returns on their investments. The following sections explore various commercial dimensions of the policy of unlinkability.

Need for personal data to conduct business

Many standard business operations require personal data. Any business transaction that concludes with a purchase will require a payment method. For electronic commerce, this means a non-cash form of payment, such as a credit card. To ensure that a person is authorized to use a particular credit card, personal information is shared in the transaction: name, address, phone number. Most often, e-commerce websites also collect email addresses from customers to communicate with them, send receipts, contact them in case of trouble, and to personalise interaction with the site. Collecting personal data in the course of business is a standard operating procedure. Some of the data collected – name, email address and phone number, for example – are highly linkable data items. The same email address given out to different merchants makes it easy, should the merchants be owned by a common parent or otherwise collude to share information, to link the transactions and behaviour of a customer. One identity management technologist observed:

> "… the currency of the realm on the internet is [the] email address." (Bob Morgan [Morgan], Interview)

Businesses are accustomed to collecting this data, and so creating and using unlinkable architectures would be a departure from standard practice (G007, Interview; Morgan, Interview; N003, Interview; Trevithick, Interview). One identity and security expert explained:

> "In general, relying parties like having more information. They are very uncomfortable when having purely pseudonymous or anonymous transactions … for account recovery or various other things that their back office systems require … they want some way of contacting or

> dealing with the user.… Pretty much none of their other infrastructure supports this perfect unlinkability or anonymity. They may not be actually trying to use the identifier to link them to information in other systems. In general, they are not, but … the software systems that they have just don't deal with the notion of not really knowing who the user is except in some abstract sense." (N003, Interview)

There are not strong incentives to change business practices in favour of unlinkability. Consumers are, on the whole, not asking for it – the drive towards unlinkability is happening in more rarefied circles, such as among policy-makers and technologists (G007, Interview; Morgan, Interview). Personal data is valuable to businesses, for marketing, internal operations, personalisation and communications (N003, Interview; N006, Interview; P001, Interview; Nash, Interview). Commercial practice militates against reducing the collection of personal information. One computer scientist noted:

> "[I]nformation is an asset … for most people, and linkages infuse that information with richness and value so the asset increases, and so we see companies with huge valuations in the market because of all the linkages they have been able to assert and collect on people." (P001, Interview)

A privacy advocate observed:

> "Businesses do not want non-correlation.…Why go to all that trouble to not know who someone is?" (N006, Interview)

Need for business cases in citizen identity management

The issues above of collecting linkable data items pertain to commercial relying parties, such as online merchants. However, business considerations are also omnipresent for private identity providers, the issuers of credentials. In the course of developing policy for citizen credentialing, federal policy-makers conceived of a set of 'use cases' where citizens would access government resources with externally-created, privacy-preserving credentials. However, building those systems is a complex and costly endeavor (P001, Interview; Nash, Interview). Processes that verify identities and then strongly bind a

person to a credential are operationally and technically challenging. FICAM policy-makers and others saw these strongly authenticated, privacy-sensitive credentials as valuable both to the American people and to the identity providers who would create and manage them. However, the for-profit companies involved did not see similar value in providing them. They did not see a clear return on the investments required to alter their systems and augment their processes to meet the government's needs (G001, Interview; G003, Interview; G007, Interview; N003, Interview; Nash, Interview).

The main divergence in viewpoints concerned credentials at Level of Assurance 2 and higher. Level of Assurance 1, which reflects little to no confidence in an asserted identity, does not require costly processes to validate a user's identity at enrolment; security requirements are also commensurately low. Most of the first group of FICAM-approved identity providers met the requirements for Level of Assurance 1 in their extant systems and therefore did not incur great costs to become certified (Nash, Interview; Wilsher, Interview). Higher Levels of Assurance were another matter. Levels of Assurance 2 to 4 require stronger identity proofing methods and increasing security requirements. This raises costs – capital expenses, operating expenses, staff time, legal expenses – and increases business risk (N002, Interview; P001, Interview). To invest in higher assurance identity systems, commercial logic demands a return on that investment. As the government was not offering to pay identity providers, the path from investment to return was unclear. A government administrator stated:

> "How do you monetise providing this service to the American people? … When you get above Level 1, we're having a much harder time with who can and will provide identity credentials." (G001, Interview)

Richard Wilsher, an identity management expert and a central figure in the British tScheme framework, remarked:

> "Level 1 was a dress rehearsal for the whole thing … [M]ost of the IDPs felt like the privacy requirements were something … they already met. So, it wasn't that difficult. Now, Level 2, Level 3 … it's like going from dress rehearsals to the real thing." (Wilsher, Interview)

Nor was there an evident demand from the identity providers' user bases. One expert recalled:

> "That's why Yahoo! and other people just said, 'Yeah, sure, we did all the technical stuff to interoperate but we are not gonna pay to get certified, that's craziness. None of our customers are asking to get in Government websites.'" (N003, Interview)

Consequently, the market for identity providers offering credentials above Level of Assurance 1 is spare. At the time of this writing, there is only one for-profit entity, Verizon, a telecommunications and business IT company, providing credentials above Level of Assurance 1. Moreover, those credentials are not for use by the general public; they are for healthcare professionals involved in the prescription and dispensing of medicines (N003, Interview; P007, Interview). The Verizon service is being offered because of a clearer return on its investments in high-assurance credentials: healthcare regulations are beginning to require the use of high-assurance credentials, creating a demand and therefore a market. Verizon sees an opportunity to make money from various parties in the healthcare field (N003, Interview; P007, Interview; Thibeau, Interview).

The business case for providing credentials to the general public has not yet been made. This is true of both credentials for e-government use, and the broader identity ecosystem envisioned by NSTIC which some see as "an unfunded wish list" (Wilsher, Interview; also see P006). So, the question remains: who will pay for high-assurance, privacy-preserving credentials for general use by the polity? The absence of a credible answer has forestalled businesses from investing in those systems. Drummond Reed (Interview) argued:

> "There is no successful system that will solve the problems of privacy and information exchange that doesn't have a successful business model. In other words … money and value exchange has to flow to offset the work that you undertake to protect information. If you've got information that's got value and it's going to flow and therefore you're going to protect it, if you have don't have a way of compensating that then you don't have a market; you don't have a sustainable system."

Andrew Nash (Interview) of Google remarked:

> "[The government is] basically saying, 'We have this enormously expensive system, we can't run it and we can't scale it. So, we are unable to deal with this, *but* we think we ought to get it for free from someone else.' This is not a very workable equation."

Multiple Markets

Many of the companies envisioned to participate in the identity ecosystem serve multiple markets, both in terms of industry and geography. To contain costs and increase sales, it behooves them to design products that can be sold across those markets, even if they have different needs and buyers. This leads to a number of effects. Firstly, identity products and services will be similar across ostensibly different sectors, such as government and enterprise. Secondly, weaker or less attractive markets will spur less commercial interest, and therefore product development, than stronger, more attractive markets. For example, the healthcare market will spur development in higher assurance credentials faster than government-to-citizen applications given the emerging demand by potential customers. Thirdly, vendors will attempt to harmonise different markets to align them with their product strategies (P001, Interview). This can happen through providing expertise to influence each market's stakeholders and clients, through consulting services or informal channels, and via influencing international standards which various markets may rely upon. Commercial companies are vital to the creation of credentials as they create and sell much of the enabling technology. Ultimately, profitability drives many of their choices, and the need to sell influences the shape of digital identity.

The drive to harmonise across multiple markets affects policy. It can potentially cause better solutions to policy problems to appear. Similarly, it can curtail policy choices. Through the conduits of transnational companies and the use of their employees as consultants and experts to government, as well participation in international standards, policy transfer can occur between different contexts and polities. For example, Microsoft, a global vendor of a variety of technologies including identity products and services, has its employees participate in a number of international standards committees on identity management (P001, Interview). Those standards can influence which technologies are ultimately brought to market. As previously discussed, available technology affects the range of implementable policies. If the standards are in fact the best possible choices, they will 'raise all ships,' benefiting the policy-making communities upstream, and those affected by those policies. If the standards favour proprietary and/or sub-optimal technologies, the range of policies may be reduced to the detriment of citizens. Relatedly, this highlights the policy effects and power of standards organizations – their efficacy, legitimacy and breadth affect the choices of policy-makers.

Variation: Higher Education

One variation to the necessity of a profitable business case comes from the domain of higher education and research. One of the first Trust Frameworks engaged with the government was the InCommon Federation. InCommon is a group of academic and research institutions and businesses related to higher education, such as academic publishers. Prior to the existence of FICAM, InCommon was a functioning federation of identity providers and relying parties. InCommon manages policies and infrastructure to allow members of a university to use their credentials at resources external to the university. This

model served as an early prototype for the use of external credentials with e-government (Morgan, Interview).

The commercial logic of for-profit companies discussed above does not apply in the case of InCommon. The mandate to build identity systems derives from higher education institutions' mission to enable access to wide ranging research resources. Bob Morgan, an identity management technologist for the InCommon Federation explained:

> "… [I]t's our overall interest in trying to improve identity management with the key customers … in higher ed. because we have thousands and thousands of researchers and all kinds of other people who have to interact with all kinds of government agencies all the time, and that just raises all the typical identity management problems." (Morgan, Interview)

All of InCommon's 330 American university members (InCommon, n.d. a), are regulated by the Family Educational Rights Protection Act of 1974 (FERPA), and those that deal in medical information fall under the Health Information Portability and Accountablity Act of 1996 (Morgan, Interview). Those two federal statues contain a number of privacy provisions regarding the safeguarding of personal data. The combination of those provisions with university enrolment, registration and billing processes allowed InCommon to be able to certify its members to a level of assurance comparable to NIST Levels 1 and 2. As in the commercial model, a potential identity provider (e.g., a university or research centre) must be audited to be certified. The number of relying parties is, at this time, small but growing, and includes grant submission through the National Institutes of Health, student loan reports through the National Student Clearinghouse, and access to scientific resources such as the Open Science Grid (InCommon, n.d. b). That said, compliance costs are not insignificant, and it is still unclear if there is enough value for universities to certify their systems (Morgan, Interview). As of September 2013, one American university, Virginia Polytechnic Institute and State

University, has been certified to the equivalent of Level of Assurance 2 (Woodbeck, 2012).

Prior to the existence of FICAM, InCommon had built unlinkability as an option into its federation (Morgan, Interview). InCommon conceived a use case where university students would log onto, e.g., an academic publisher. Inheriting some ideas regarding privacy from the Liberty Alliance, InCommon administrators felt that it was not necessary (and could possibly trigger FERPA considerations) for student names to be sent to the publishers; all that needed to be sent was an assertion that the student was, in fact, a member of the university (Morgan, Interview). This led to the use of 'transient identifiers' – a pseudonym that would only last for an individual session. The assertion from the university contained this identifier, which held no personally identifiable information, and an attestation that the user was a member of the university, and was therefore allowed to access the publisher's resources. By using the transient identifier, a publisher or other relying party would be less able to build a profile of a student's other online activity. Other use cases exist, however, such as collaboration on research projects with common sets of resources. In those cases, email addresses and other linkable identifiers are shared without issue. Given the variety of interactions, system designs and organizational needs, unlinkability is but one tool in the "tool kit" of federation technology (Morgan, Interview).

When Linkability is Good

In addition to the commercial value of linkages to both identity providers and relying parties, linkability benefits data subjects. Facebook, with a (self-reported) user base of over 1 billion people at the time of this writing (Lee, 2012; see also Tavakoli, 2012), has built its business around linking the habits, attributes and online activities of its members. Much of the data it collects is volunteered by its members who spend millions of minutes per day on

Facebook. The growth of social networking and other recent internet business trends has relied on the linking of personal data and online activity (David, Interview; Morgan, Interview; P003, Interview). One computer scientist observed:

> "… it's the linkability of particular kinds of data which has been responsible for so much innovative and new services that people are benefitting from…" (P001, Interview)

Another beneficial example is fraud detection. The linking of various transactions in both the online and offline world helps financial companies detect, for example, if credit cards are being used fraudulently. Andrew Nash explained:

> "If you have a conversation with somebody and say, 'Do you want the credit card companies to track your information?' The answer is, 'Hell no.' However, if you say, 'Look, an anomaly occurred or something went wrong in my credit …' do people want to be able to see an audit trail of their transactions? And the answer is, 'Absolutely.' And so the two of those are in conflict, but anybody that's had an issue with their credit suddenly finds that you know they want to know what's going on." (Nash, Interview)

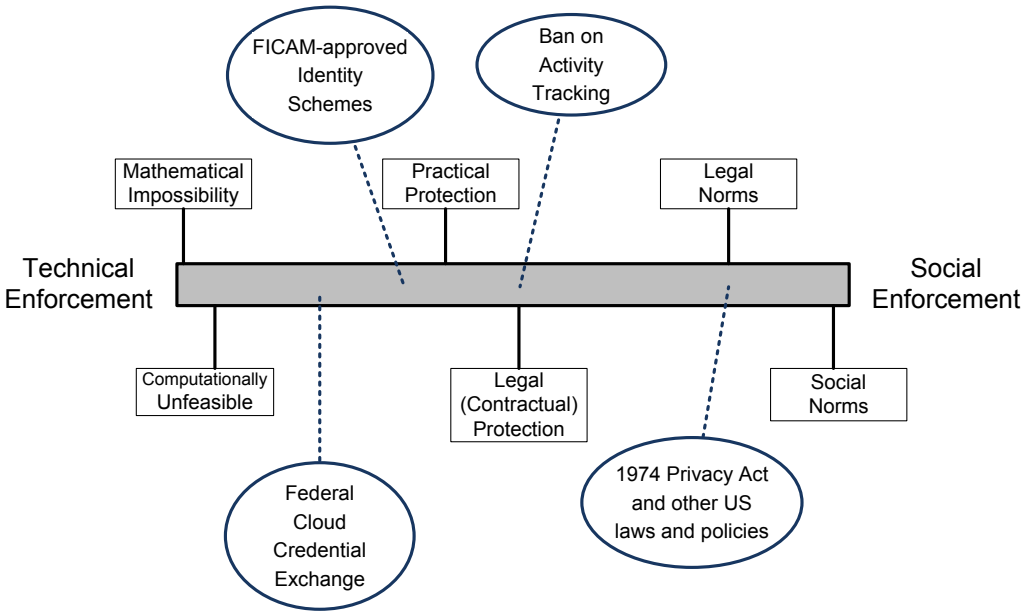
One of the earliest use cases envisioned by the US government provides another example. Identity management goals from the early 2000s included an intention for Americans to be able to sign up for national park resources via the web (OMB, 2002). This could be done pseudonymously – assigning a number to a campsite reservation that a person could obtain without revealing her identity. However, it benefits the person to supply an email address in case something goes wrong with the reservation, or a weather event forces a closure of the campground.

Technical vs. social methods of privacy enforcement

As noted above in Drummond Reed's spectrum, a consideration of unlinkability as policy illustrates different methods available to policy-makers

to preserve privacy. The evolving efforts of the US government appear at multiple points on Reed's spectrum.

Figure 5.5 US IDM privacy efforts in relation to Reed's spectrum



On the technical side, there is a requirement for identity providers to issue different pseudonyms for each relying party when using the SAML protocol. The proposed Federal Cloud Credential Exchange, essentially a technical layer that can, among other things, enforce privacy policies, will also fall to the left of the spectrum. Towards the social side is FICAM's Activity Tracking restriction, preventing identity providers from using or divulging information about a user's online activity. Further right, Federal agencies are legally restrained from collecting more information than they need, including information on someone's unrelated online activity (G006, Interview), by the Privacy Act of 1974 and other policies.

To use technology as a regulatory mechanism for privacy policy enforcement requires both that the technology is feasible and that there is a sufficient

business case for the technology to be deployed. For example, the OpenID standard that the Federal CIO wanted to be used for citizen credentialing was not, at the time, capable of providing a pseudonymous identifier dynamically, i.e., upon request by an agency (N003, Interview). The standard had to be modified to meet FICAM's privacy requirement. SAML, the other federation protocol, had the same problem, but the standard could not be modified as easily "[b]ecause there was no perceived need in the SAML community" (N003, Interview). OpenID implementations were 'home grown' and able to be configured to a very granular degree by an individual identity provider, but SAML implementations are underpinned by commercial software packages whose features are controlled by their vendors. Changes in the protocol would need to 'propagate' into the software packages, which the vendors were not required to do. A senior identity management standards developer noted:

> "So most large OpenID providers … are using their own implementations, so getting them to make the required modifications versus … trying to deal with Oracle and Sun and Computer Associates and various other folks to attempt to get them to put the software to make this change without customers demanding it … Large software vendors, unless there's [*sic*] customers waving money in front of their faces, good luck." (N003, Interview)

This is another example of the need for a business case to meet privacy goals in the online world. Since government is relying on industry to provide large-scale identity management solutions for the public, its policy goals are constrained by both the state of the art of technology, and the commercial needs of the vendors who bring those technologies to market. It is the 'business of privacy protection.' "[M]aking a system anonymous and unlinkable is genuinely more complicated, therefore more expensive" (P001, Interview). Given the costs involved, it is still unclear whether companies who build identity technologies will have a reason to make them as privacy-preserving as some hope. The senior standards developer reported:

> "…the reality is that abstract claims in an unlinkable way have a really narrow use case … people spread around their correlatable identifiers willy-nilly using their email addresses … as their usernames to log into sites without thinking twice about it … While it might be nice to have theoretically unlinkable claims, there is no commercial marketplace for that. Without a business case, it's gonna be hard to … get people to change the way they they're heading." (N003, Interview).

Privacy at the protocol level

The issue of feasibility above highlights the role of protocols in online privacy. The internet is built on a wide array of standards – agreements between interested and/or official parties on the rules of a given system – and protocols – implementations of those standards into methods of communication (Tanenbaum, 1996, p. 17). Identity technologies such as SAML, OpenID and others are useful because they are standardised – different vendors and customers can all talk to one another reliably. However, in the case of a small pool of available standards, technical choices can become limited. Where policy requires a technical component, policy choices may be constrained by technical limitations. Standards and protocols therefore have power.

> "You really can't separate the technical from the policy because the policy is implemented in the code." (N002, Interview)

In the cases of OpenID and SAML noted above, the standards were not capable of meeting government policy objectives without modification. Some of the real-time notice and consent characteristics envisioned by government administrators and policy-makers are still not feasible in currently deployed identity technologies (G001, Interview; N003, Interview; N004 Interview). The degree to which the standards can be modified is reliant on the caretakers of those standards, the standards development organisations, related interested parties, and the accompanying commercial environment. Thereby, standard development organisations are, in effect, actors within a policy community.

They, too, hold power, and are vital components in the landscape of privacy protection on the internet. An identity management expert observed:

> "Having privacy as an ideal doesn't do you any good unless you got folks that are coding to it…" (N002, Interview)

The role of standards developers' norms and values is explored at length in Chapter 8.

The challenge is not technical

The difficulty of preserving privacy in the online world generally and the identity space specifically is not a technical one (David, Interview; Reed, Interview). Cryptographic tools, while possibly lacking in the consumer market, are well understood and mature. Identity standards are maturing and have robust communities of interested parties. There are certainly challenging issues of usability (discussed below), but the actual technology needed to protect data from unwanted gazes exists in a variety of forms. The challenges are economic, as described above, and ultimately social in nature. Scott David, an expert in contract law for identity management and Executive Director of the Law, Technology & Arts Group of the University of Washington's School of Law, remarked:

> "I think that we have been rowing with one oar in the water by trying to find technical solutions only to these issues.… [T]hese are social systems, not technical systems, and they need social solutions, and social solutions are solutions of norms and behaviour." (David, Interview)

Comparability vs. compliance

By engaging the private sector through the policy and procurement mechanism of Trust Frameworks, the federal government set aside the traditional notion of compliance. By relying on an external third party to assess private sector actors against their published requirements, the government had to accept *comparable*

policies to their own, rather than an adherence to a compliance regime. This is because the government was abstracted from the private actors and was, in effect, outsourcing an element of its policy-making. A government official explained:

> "The whole idea the Trust Framework provider process is to abstract federal Government from trusting individual IDPs." (G004, Interview; See also Greenwood, Interview)

An identity management expert noted:

> "[Comparability] means that if you're trying to add up to six, you can have a three and three, or you can have two and a two and a two, you know, you can get there [by] various ways." (N002, Interview)

The main reason for pursuing comparability versus compliance was to relieve the government of the burden of certifying identity providers (G003, Interview; G004 Interview; N002, Interview). By inserting a non-governmental third party, the overall ecosystem for credentials is made more scalable. More Trust Frameworks with different Assessors could be added to the ecosystem without the government needing to restate its own policies. More IDPs could become approved to interact with federal agencies without additional certification overhead for the government.

Comparability is a form of 'translation' – government policies are translated by the Trust Framework Provider and its independent assessors. The reinterpreted policy, now abstracted from its source, is then applied to identity providers. Official government policy becomes thus localised. This is true for the operational components of FICAM, though the technical requirements behave more like compliance. Technical interoperability has less flexibility than other processes – IT systems on either end of a credential exchange process have to be configured to understand and comply with one another by conforming to the published schemes. Therefore the technical dimension of unlinkability – e.g., the use of pseudonymous identifiers – is able to avoid becoming reinterpreted

as the original policy is more directly testable. The Identity Scheme Adoption Process (ICAM, 2009a) was used as a way to ensure close adherence to the government's policy intentions. An official explained:

> "The scheme is a way of defining options in such a way that allows interoperability within the broad standard range.… The value of the government management in that particular case was that it enabled interoperability within the conceptual universe of the policy. And to the extent that anyone wants to play in that universe, you know what to do and how to do it." (G004, Interview)

The translation character of comparability is well-illustrated by the publishing of FICAM's privacy requirements. Kantara, one of the four approved Trust Framework Providers, accredits Assessors who audit companies that wish to be identity providers to the government. Those Assessors determine if the applicant company has comparable operational policies and are technically interoperable with FICAM's published protocol Schemes. They also ensure that the applicant meets FICAM's privacy requirements. Those requirements were published in the Trust Framework Provider Adoption Process. However, the Assessors are accredited by, and effectively work under the aegis of, Kantara. In order to make the privacy requirements auditable, Kantara had to 'internalise' them. They created a Federal Privacy Profile (Kantara Initiative [Kantara], 2010) that aligned closely with the FICAM privacy requirements (N004, Interview; Wilsher, Interview). FICAM administrators were shown and approved the Profile. Kantara's interpretation of the privacy requirements into its Profile and the subsequent localisation of the requirements by Assessors illustrate the breadth of policy actors within identity management.

Actors

A central figure in the various iterations of identity management policy for citizen access is a consultant named Chris Louden. He and his associates in a company called Enspier, later acquired by Protiviti Inc. (Wilsher, Interview),

were present for some of the earliest iterations of citizen-focused identity management (P006, Interview). They were integral to the government's thinking regarding the privacy architectures in the Electronic Authentication Program and then FICAM (G004, Interview; N002, Interview; P006, Interview; Wilsher, Interview). One administrator recalled:

> "Chris is the primary intellectual architect.… Chris is the brains behind the technical side of the operation." (G004, Interview)

Enspier also helped draft the Office of Management and Budget's memorandum which laid out the Levels of Assurance methodology and NIST's electronic authentication guidelines (P006, Interview). Mr. Louden was partly responsible for the government requirement for identity systems to support pseudonymity. One engineer remarked:

> "… the intent was to try to minimise the amount of information. So, one of Chris's philosophies was, and it sounds somewhat trite, but 'less is more.'" (P006, Interview)

Enspier's role illustrates how consultants are part of a policy-making community, and can have long-lasting and wide-ranging effect on matters that affect an entire country. Mr. Louden and his colleagues' contributions to US government efforts are part of the story of the evolution of US privacy through non-legislative means.

Usability

A consistent theme within the case is the usability of identity management systems: unless identity management systems are easy to use, people will not use them. A computer scientist noted:

> "There's a huge issue around usability that if you can't address the usability concerns then … even if you have great technology, people won't use it right. They'll make silly mistakes and it won't work." (P001, Interview)

Some believe unlinkability to be conceptually difficult for users (G007, Interview; Morgan, Interview; N006, Interview; P001, Interview). While people may have facility with pseudonymity in the physical, social world, the use of identity credentials is obscure. The computer scientist observed:

> "… the mental model is not something people are used to seeing in terms of identity providers, relying parties, intermediaries, it's really complex and we need the average person to be able to embrace these in a way that they get intuitively and it's just a very big step, it's gonna take a while." (P001, Interview)

One privacy advocate echoed this observation:

> "[N]ormal people don't think of their identities as disjointed, at least not yet … [Y]es, [unlinkability is] the right thing to do from a … long-term privacy protection [perspective], but industry doesn't want it, and normal people don't get it." (N006, Interview)

Further, the invisible nature of electronic communications causes identity management systems to need a degree of clarity that is, so far, challenging to system designers (N005, Interview). Technologists and policy-makers in the identity management community are aware that 'burdening the user' with an overabundance of choices and information does not help (G001, Interview; G007, Interview; N004, Interview). 'Notice and choice,' a concept rooted in the Fair Information Practice Principles and other privacy and data protection instruments, can sometimes have the opposite intended effect. Continual notifications about what information is being sent to whom, repeatedly asking a user if she consents, or which pieces of information should or should not be sent leads to "user fatigue" (G001, Interview). A government administrator stated:

> "… one of the issues we always deal with, and that our privacy people are actually very aware of, is if you build in too much choice, usability gets crushed. … people get confused and overwhelmed and they attempt to run away and tend to think that something bad is happening.…" (G007, Interview)

There is some concern that the goals of notice and choice – transparency, informed consent, and autonomous participation (Sloan and Warner, 2013) – will be hindered by deluging users with too much information; that users will become trained to click through without reading (G001, Interview; G007, Interview; Morgan, Interview; N004, Interview). One identity management expert expanded on this point:

> "So we know that users have been trained to click through consents and … notices, which does not make them useful, valuable ... It does not make it something that you can regulate against if you can't prove … that the user actually understood what it was that they were doing … [I]f they know how their information [is] intended to be used or potentially may be used, then they can make a choice in terms of their own privacy. If they don't understand these issues, then they can't really make a choice as to whether they want to participate in a system or not." (N004, Interview)

Privacy introduces 'friction' into online transactions. That is, privacy goals, such as transparency, notice, consent, choice, user participation, and security goals like strong authentication usually require that an additional step is introduced between a user's actions and his desired outcome. Entering a password is a necessary step that intervenes when a user tries to access a resource. Informing a user which information will be sent to a relying party pauses a transaction. Asking a user to consent to the transmission of her personal data interrupts her activity. Given the conceptual difficulties of identity credentials, this friction can undermine the best intentions of system designers and regulators. Paul Trevithick, an identity management standards developer and founder of the Information Cards Foundation, observed:

> "… [E]verything about privacy/security is nothing but new friction to be introduced between you and what you want to achieve on the web. So, I know commercially that's the struggle." (Trevithick, Interview)

One privacy advocate echoed this:

> "… it is very difficult to tell consumers in an iPhone age when people actually want slick frictionless services and don't want to have to read

> and think and make decisions lot of the time – some people do, many people don't. Asking companies to be clear about their notices, clear about their consent while still providing a product that is user friendly is a difficult balance." (N005, Interview)

Besides the additional steps and conceptual difficulties, it is unclear if users care about the privacy goals in identity management systems (G007, Interview; N005, Interview; N006, Interview; Trevithick, Interview). The ostensible harms of profiling are invisible to the user. A privacy advocate remarked:

> "It's hard to get people to care about something they can't see unless they have a reason to feel uncomfortable about it…. I think finding incentives for unlinkability are difficult because it's invisible to most people unless you misbehave … or not even misbehave." (N005, Interview)

Nor are relying parties necessarily inclined to do the additional work required to create unlinkable systems. Bob Morgan noted:

> "… [I]f you're a physicist putting up a website, the fine distinctions between the … opaque unlinkability identifiers and regular user IDs and transient IDs and all that stuff … it's like, 'Don't bug me,' right? 'I just want to know who the person is.'" (Morgan, Interview)

There is agreement among the respondents that giving users choice – to be pseudonymous, to send certain kinds of data – has great value, but that doing so in a meaningful way is difficult (Morgan, Interview; N005, Interview; P001, Interview). A privacy advocate opined:

> "I think user control is one of the only stable places to hang your hat when you're talking about privacy … you can offer a service, you can offer almost any service you want, as long as it's not just unconscionable. But you got to give people choice as to whether or not they want to engage in that sharing of their information… I think there is an inevitable tension between robust notice and choice stuff and frictionless user friendly stuff." (N005, Interview)

A computer scientist observed:

> "So even though there's a tremendous desire to empower people with control for privacy, it's still very tricky … with … a user-centered architecture or … minimal disclosure [technology] … in the hot seat [to enable] a person [to] make the right kind of tradeoffs and decisions that they need to make to protect themselves." (P001, Interview)

Usability issues are critical to achieve the goals of greater user control and to ensure the effectiveness of privacy technologies in the identity management space. The 'user-centric' design movement in technology is a broad heading under which such issues can be addressed (Leenes, 2008). The data in this chapter underscores the challenge of user-friendly designs in IDM. Research on ideal types of privacy-preserving IDM systems has occurred in Europe under the PrimeLife project (PrimeLife, n.d.). Future research into IDM policy could fruitfully apply the usability lessons learned in PrimeLife (Graf, et al., 2011) to national citizen credential initiatives, such as the UK Identity Assurance Programme and the interactions via the German AusweisApp (see Chapter 6).

Conclusion

This chapter detailed the empirical data gathered on the US policy of unlinkability. To do so, it explored in depth US identity management policies for citizen credentialing. These policies were born out of e-government authentication needs in the beginning of the 2000s, and were driven exclusively by the Executive branch. Rather than issue its own credential, the US government elected to obtain credentials from private organisations to enable citizens to authenticate themselves to e-government resources. This is due in large part to a strong, historical antipathy towards national identification, as well as the size of the US population.

The choice to use externally-created credentials necessitated the creation of a risk management framework to harmonise federal agencies' ability to judge the

credentials' validity. An intermediate party known as a Trust Framework was inserted between agencies and private identity providers to ensure that the providers' technical, operational and privacy practices were comparable to the federal government. Privacy rules were encoded into operational guidance and within technical protocols – a mixture of social and technical methods of enforcement. In extant credentialing initiatives, identity providers are recommended or required to use unlinkable pseudonym identifiers depending on the underlying technology. A recently proposed national identity management system, the Federal Cloud Credential Exchange, requires stronger unlinkability and will rely on technical enforcement to a greater degree than current policy. When built, it will be one of the largest unlinkable credential architectures in the world. Current and proposed US citizen IDM systems are an example of PETs as policy.

Unlinkability was added to US identity management policy by consultants and privacy practitioners. In the former case, a belief in the virtue of data minimisation led to unlinkability's inclusion in the technical architecture of early IDM efforts. As policy developed towards an initiative that would cover the whole of the US population, privacy officials reinterpreted the Fair Information Practice Principles, a non-binding set of principles that underpin much of US privacy policy. This reinterpretation plus an application of a 1974 federal privacy law contributed to the inclusion of unlinkability requirements for citizen credentials. These requirements serve the privacy interest of separating informational contexts, despite the fact that, unlike Germany, there is no strong mandate in US law to do so.

Citizen IDM systems, particularly in the US, are subject to commercial influences. By relying on privately-issued credentials, the government's policy intentions are bound to market logic. This is evident in the lack of interest by private issuers to supply credentials to the American public due to the lack of a

compelling business case. As a result, US policy intentions have been hindered, and there are no high confidence digital credentials available to the general citizenry.

CHAPTER 6: UNLINKABILITY IN GERMAN INFORMATION POLICY

Introduction

This chapter details empirical research on the appearance of unlinkability in German information policy. In order to explore this process, the chapter examines the genesis of the German electronic national identity card (e-ID) and its privacy features. The e-ID is a 'path continuation' (Noack and Kubicek, 2010) of the prior paper national ID, and was brought into existence by a specific law, the *Personalausweisgesetz*. This law specified a data protection model, and subsequent technical guidelines based on the law required the e-ID to be able to produce pseudonyms on a per-relying party basis. The logins based on those pseudonyms, in the absence of other linkable identifiers, are unlinkable. Further, the German e-ID system as a whole is 'unobservable' from the perspective of the identity credential issuer, the state. These policies and architectures are an example of privacy-enhancing technologies as public policy.

Germany was chosen as a case for this thesis for several reasons. Firstly, an initial literature review indicated that the German e-ID produced pseudonyms, which was evidence that unlinkability may have been a policy choice. Secondly, Germany has a federal government, and the e-ID originated with a federal agency, the Ministry of Interior. This supported a most similar systems design for a comparative case study given that the US was also federal, and its citizen identification initiatives originated at the federal level with the Executive branch. The key difference between them was that the German state was issuing digital identities via the e-ID whereas the US sought externally created identities for its citizens via private organisations. This difference was analytically rich, illustrating the powerful differences between market forces and government logics. Both countries have institutionalised data protection,

but this manifests differently in each. Data protection and privacy in the US at the federal level derives from a variety of sectoral laws and policies, and is partly guided by a non-binding set of 'Fair Information Practice Principles.' In Germany, an omnibus data protection law covers all instances of 'personal data.' This law is a transposition of the European Union's Data Protection Directive which Germany was required to enact under the terms of its membership in the Union. The EU also requires that Germany have a data protection authority to ensure appropriate application of relevant policies (European Council, 1995, Art. 28) – these exist at both federal and state levels. Neither the omnibus conception of personal data nor a data protection authority 'layer' exists in the US. Still, unlinkability is appearing in both countries, partly because of commonalities between the US Fair Information Practice Principles and the EU Data Protection Directive (Gellman, 2012).

The data in this chapter is drawn from fourteen interviews with key actors related to the policy of unlinkability and the creation of the German e-ID. Interviews were conducted with Jan Möller, a lawyer at the Ministry of Interior and a principle author of the *Personalausweisgesetz*; four members of the Unabhaengiges Landeszentrum fuer Datenschutz (ULD), the Independent Centre for Privacy Protection in the state of Schleswig-Holstein, including their Deputy Director, Marit Hansen; Jens Fromm of the Fraunhofer Institute; Prof. Dr. Herbert Kubicek of the Institut für Informationsmanagement Bremen; Prof. Dr. Gerrit Hornung of the Universities of Kassel and Pasau; and other government officials and scientists. See Appendix A for a complete list of all interview subjects and sampling rationale. Data was also drawn from primary and secondary documentation, including laws, policies, technical guidelines, academic literature, blogs and the press.

The first half of the chapter is a policy history of the e-ID, and covers the core policy intentions and reasons cited for creating it. Like the US case, e-

government initiatives are interwoven into the history and reasons for citizen credentialing. The e-ID's features, user interaction and data protection model are explained, including an in-depth examination of its pseudonymity capabilities, which are most relevant to understanding unlinkability in the German context. The second half is an exploration of emergent themes within the data: informational self-determination, the German privacy 'mindset,' stronger protection of validated data versus volunteered or commercially obtained data, the e-ID's relationship to the electronic passport, the commercial dimension, technical versus social methods of privacy enforcement, marketing, the actors involved and usability considerations. The themes were derived of primary and secondary documentation, from repeated appearance within the interviews, and from induction. Themes are selected and presented in order to highlight the key issues relevant to explaining the policy of unlinkability (McClure, et al., 1999; Braun and Clarke, 2006). Some of these themes have been explored in relation to the US case data, and some are new, particular to German history, culture, law and policy implementation.

Overview

A new German e-ID card was rolled out in November 2010, replacing the larger paper one. The e-ID holds all of the same data as its predecessor plus post code, and stores all of that information on a chip inside the card body. By virtue of its electronic components, the card enables a number of privacy-friendly features and can be used to authenticate citizens over the internet. The data protection regime and culture affecting the e-ID derives in large part from a seminal Constitutional Court case in 1983 that defined a broad set of rights for German citizens over their informational lives. E-government initiatives and other factors spurred the creation of the e-ID, taking approximately five years from the first public disclosure of the plan to deployment. However, due to poor marketing, a lack of perceived value, and a low number of websites that can access the card, less than one third of all cards have their online

authentication feature turned on (DE-G002, Interview; Jens Fromm [Fromm], Interview). Due to a 10-year card validity, both for the original and electronic ID, all German citizens will possess an e-ID by 2020, making it the largest national electronic ID infrastructure in Europe (DE-G003, Interview). As such, it will also be one of the largest examples of unlinkable credential architectures in the world because of its pseudonymity features and the size of the German population.

E-government Initiatives

The German federal and state governments began to experiment with e-government services at the end of the 1990s (Breitner, 2003, p. 12). In 2000, the federal government launched BundOnline2005, a broad programme intending to put all federal public services online by 2005 (IDABC, 2009, p. 8; Noack and Kubicek, 2010, p. 89). Many German public services required residents to sign forms; the signature served as the authentication necessary to ensure that the citizen was whom he claimed to be (Noack and Kubicek, 2010, pp. 88-90). As paper documentation was moved online, electronic signatures were seen as critical to the success of these early e-government efforts. This led Germany to promulgate an electronic signature law two years before the 1999 EU electronic signature directive (Noack and Kubicek, 2010, p. 89). However, electronic signature technology was both costly and nascent, and there was little use of it by the citizenry (Jan Möller [Möller], Interview). More importantly, electronic signatures contained insufficient information to identify and authenticate individuals uniquely (Noack and Kubicek, 2010, p. 89; Kubicek, Interview). To obtain an electronic signature certificate, a citizen needed to show proof of identity. Despite this, because of the lack of information in the certificate, two people with the same name could not be distinguished by an entity receiving electronic signatures (IDABC, 2009, p. 6; Herbert Kubicek [Kubicek], Interview). Government officials in charge of evolving German e-signature law "maintained that a handwritten signature also

consists of surname and first name with no additional attributes and therefore saw no need to add any other attributes in the digital word" (Noack and Kubicek, 2010, p. 90). Ultimately, government administrators and technical personnel recognized the insufficiency of e-signature as an authentication tool. In 2003, revised plans were sought for appropriate ways to authenticate citizens in e-government interactions. By 2004, electronic ID cards were being discussed within the Ministry of Interior, and had come to be viewed as the only suitable token for e-government authentication given the insufficiency of e-signatures (Noack and Kubicek, 2010, p. 91**)**. This time, the system would be designed specifically to separate legal intent (signature) from authentication. Not only would this correct the mistaken use of e-signatures for identity verification, but it would also mirror practices in the physical world with paper ID cards. That is, displaying an identity document in a face-to-face interaction does not leave a 'trace'; the interaction itself is not verifiable without additional information. A signature, however, is an attestation of legal intent meant to be provable in the future. Government officials specifically sought to separate these two situations in the electronic ID. One government scientist explained:

> "… [W]hen I show you my identity card you can see that I'm the legitimate holder of it. You can see my picture, you can see my name, my date of birth and… all my personal details on it but you can't prove it to any third party. With an … electronic signature mechanism as an authentication, you send me a form requiring me to sign [it], and afterwards you are able to prove to everyone that you received my signature.… So you can prove that we had some interaction. That is something which we wanted to prevent, and that was the reason why we came up with some purely authentication function with a pseudonym behind it and that's all. That was the starting point: clearly separating authentication and, we call it 'transactions.'" (DE-G001, Interview)

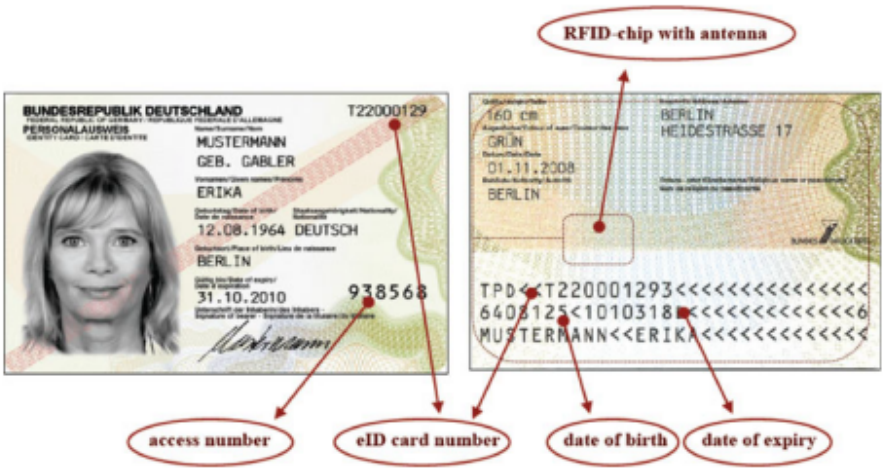
Introduction of the e-ID: Policy history, rationale and intentions

In 2005, the Ministry of Interior released its "e-card Strategy" (Schmidt, 2005; ULD, Interview). It envisioned the creation of an electronic identity ("e-ID") card to replace the existing paper laminated identity card (see Figure 6.1 below), a health card for use with national health services, and an electronic passport ("e-passport"). The new e-ID, the *neue Personalausweis* (see Figure 6.2 below), would serve as a traditional official identity document as well as a travel document within Europe in lieu of a passport. European law requires member states to accept national ID cards as border documentation. The proposed e-ID would optionally have the ability to create electronic signatures, as well as allow cardholders to authenticate themselves online.

Figure 6.1 The original paper laminated national ID card

Source: Noack and Kubicek, 2010, p. 97

Figure 6.2 The new e-ID card



Source: Noack and Kubicek, 2010, p. 98

Soon after the Interior Ministry's announcement, the Ministry hired Jan Möller to work on the e-card project. Mr. Möller had worked for the prior four years at the Unabhängiges Landeszentrum für Datenschutz (ULD), the Independent Centre for Privacy Protection, the data protection authority for the German state of Schleswig-Holstein (Möller, Interview). His experience working at the ULD would help shape the privacy characteristics of the e-ID, discussed further below. The Ministry also began to engage federal and state data protection authorities and privacy experts. The chief discussion point within the Ministry and the German Parliament was the inclusion of biometrics on the card (Gerrit Hornung [Hornung], Interview; Kubicek, Interview; Möller, Interview; ULD Interview). The card's privacy features were otherwise accepted with little debate. Gerrit Hornung (Interview) recalled:

> "… [T]he federal data officer made a strong claim against the fingerprints but on the authentication mechanism he said, 'Well, I've looked into that and it's technically sophisticated, it's data protection friendly, so I'm happy with that.' So he sort of made strong statements on biometric side and that was what the political debate focused on then."

The new e-ID was intended to mirror the original national ID. This meant holding the same data that was printed on the original card, including the holder's photograph. The e-ID would show the data on its printed surface and contain the same data on an internal chip. Initially, the Ministry wanted the e-ID to also mirror the e-passport meaning the mandatory inclusion of digital images of the cardholder's fingerprints (ULD, Interview). Various data protection authorities objected to the mandatory inclusion and ultimately fingerprints became optional. The fingerprints are not stored in centralised databases – this would contravene German law (Hornung, Interview). They exist only on the cards themselves and the federal printer is required to delete them after card production (DE-G001, Interview; Hornung, Interview; ULD, Interview).

In November 2010, the e-ID card was released to the citizenry at a cost of €28.80 each. The following year, the Ministry released the *elektronischen Aufenthaltstitel* (eAT), an electronic identity card for non-European residents. The eAT mirrors the e-ID identically plus additional data fields indicating residence status (DE-G003, Interview).

A number of reasons to develop the new e-ID were cited by official documents and interviewees. The e-ID's size was a factor (DE-G001, Interview; ULD, Interview). The original national ID was in the ID-2 format: 105 × 74 mm (4.134 × 2.913 in). The new e-ID would conform to ID-1, 85.60 × 53.98 mm (3.370 × 2.125 in), the international standard used for credit and banking cards and the other electronic ID cards appearing in Europe (DE-G001, Interview; ISO/IEC, 2003). There was an intention to improve the security of online interactions by providing citizens with a hardware token to replace the use of username and password (Horsch and Stopcynski, 2011, p. 1; Noack and Kubicek, 2010, p. 99; DE-G001, Interview). This would allow for 'two-factor'

authentication: possession of the card plus use of a password. One computer scientist explained:

> "The main idea behind the authentication with the identity card in the internet was to provide an alternative to username / password… So from a one-factor authentication, like only knowing a password for a certain account, we wanted to have a two-factor authentication, so to make it more secure. That was a basic idea." (DE-G001, Interview)

Since the card was an official form of identification and its enrolment procedures were trusted by government, the Ministry of Interior created the capability to authenticate the bearer online. More broadly, there was a desire to enable German citizens to use their identity on the internet. Jens Fromm, a scientist at the Fraunhofer Institute who was closely involved with the development of the e-ID, stated:

> "… [I]t is the wish of the German government that every person, every citizen has an electronic identity through his German identity card with certain attributes with certain personal data so that he or she can use it for transactions in the digital world. So this was really five years ago one of the reasons why the German government decided to push forward this electronic identity function." (Fromm, Interview)

From the beginning, the authentication feature was intended for use with both e-government applications and commercial ones (Schmidt, 2005; Fromm, Interview; Möller, Interview). Officials understood that a pure e-government focus would be insufficient because the relatively low number of citizen-government interactions would not allow a person to acclimate to using the card online. Jan Möller stated:

> "The whole concept was it's open to e-government and private. The main reason is that the average contact rate of a German citizen to administration is 1.8 a year, and if you have a technical process, you need some exercise that you know how it works. If you do something just once a year, you don't get used to it, and something like that only works if you get used to it, so we needed more situations when people actually need it." (Möller, Interview)

The cost of the card to the citizen was approximately triple the price of the original ID card. The online authentication function was seen as a way to increase the value of the card to the citizen, in part justifying the higher cost (Möller, Interview). The card could also produce electronic signatures, and was hoped to encourage greater citizen use of them. The e-signature function requires privately obtained certificates to be loaded onto the card. At the time of this writing, the signature feature is dormant in all e-IDs because of a lack of business interest in selling the necessary digital certificates. This is because the e-ID signature function would compete with established e-signature products (DE-G003, Interview).

Features

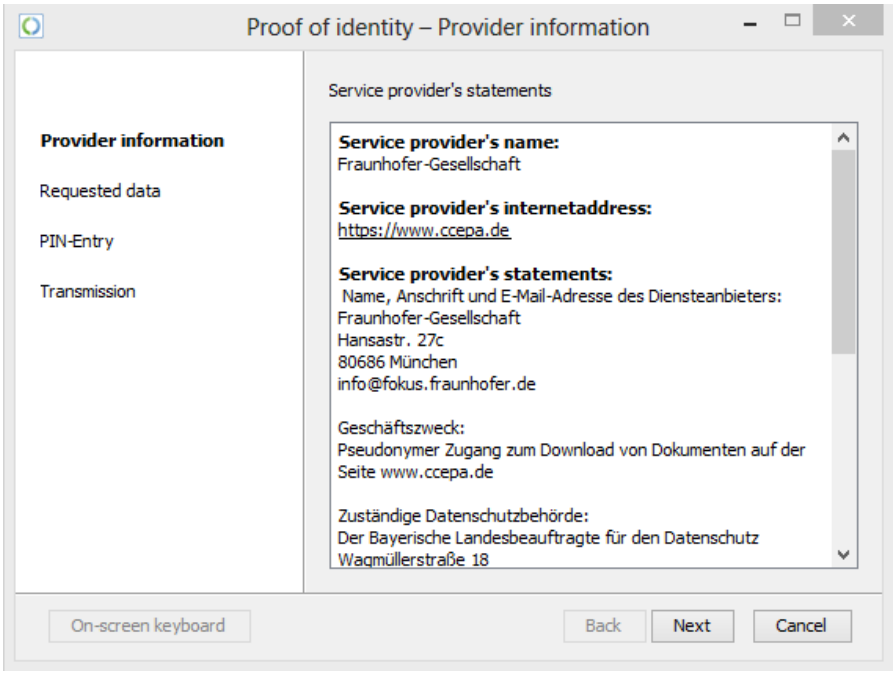
The *neue Personalausweis* contains nine data fields printed on its face and stored on its internal chip: first name, surname, birthdate, place of birth, doctoral degree, current address, post code, municipality ID, artist/religious name, and expiration date (Poller et al., 2012). It has a photograph of the bearer printed on its face and stored digitally in the chip. Optionally, two fingerprints can be stored in the chip as well. There is no current application that uses the fingerprints (Hornung, Interview; ULD, Interview). The card is contactless – it relies on radio frequency identification (RFID) technology to communicate with a reader. The card is capable of performing three mathematical functions. First, the card is capable of responding Yes or No to the question of whether the bearer's birthdate is before or after a particular date. An application can query if the bearer is, for example, between 16 and 35, or over 18, and the card will respond with a Yes or No. This feature is called 'selective disclosure'. There is a similar capability with current residence. German regions are hierarchically divided from state to municipality, and the card is able to respond Yes or No to questions of which region does the bearer reside in. The third mathematical function is related to unlinkability – the card is capable of

producing pseudonyms. To fully explore this privacy feature, explanations of the e-ID's user interaction and data protection models are required.

User interaction

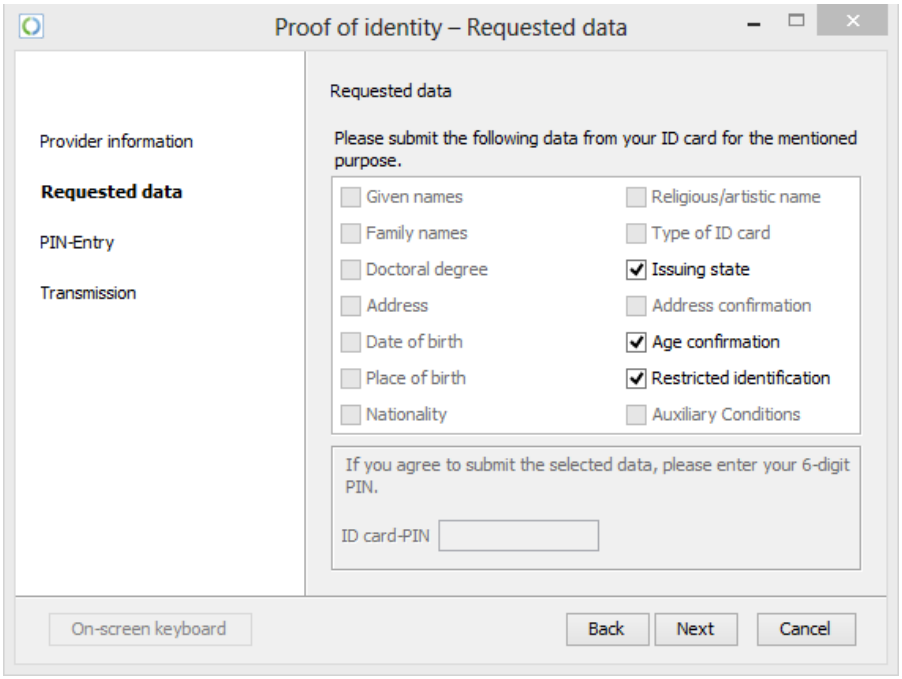
The primary use of the e-ID is as proof of identity in a face-to-face interaction. The secondary use is to authenticate the bearer online. The online model is a two-party interaction between a service provider and the cardholder. A service provider is any web-based entity: agencies that manage e-government applications, or private businesses. The online use case is a citizen accessing a website that needs validated proof of the citizen's identity. When the citizen goes to the website, she places her e-ID on a reader attached to her computer.

Figure 6.3 AusweisApp screenshot: requesting service provider information



Source: Ministry of Interior, personal communication

Figure 6.4 AusweisApp screenshot: requested personal data



Source: Ministry of Interior, personal communication

A piece of software called the AusweisApp launches and the citizen is shown contact details for the requesting entity and the data fields requested. Above are two screenshots in English of the AusweisApp showing the service provider details screen and the requested data screen. If the citizen agrees to send the data, she enters a personal identification number (PIN). The data is sent and the main transaction continues.

Data protection model

The law that brought the new e-ID into existence, the *Personalausweisgesetz*, requires service providers to transmit an authorisation certificate to the card in order to get access to the data on the e-ID (Zwingelberg, 2011, p. 151-154; DE-G002, Interview; ULD, Interview). To obtain the certificate, service providers apply to the Bundesverwaltungsamt (BVA), the Federal Office of Administration, a sub-agency of the Ministry of Interior. Service providers

must make a case for the specific data fields and functions they wish to access. For example, if a company wished to obtain first name, surname and birthday, the company would have to justify its needs for that personal data based on its business model and the needs of its web application. Administrators at the BVA review all applications and judge whether the request is justified. The judgment is based on the 'principle of necessity' – whether the service provider actually needs the data or not – as well as the principle of data minimisation, requiring that only the minimum information be sent (Zwingelberg, 2011, p. 151-154; DE-G003, Interview). If an applicant is approved, it presents this legal authorisation to a private third party to obtain a technical authorisation, a cryptographically signed certificate bound to the applicant organisation. The certificate contains the legal authorisation, the name of the organisation's data protection authority, and a list of all of the data fields the organisation has been given the right to access.

When the cardholder uses the AusweisApp, it displays all of this information on her screen prior to entering her PIN (see Figure 6.3 above). In this way, the citizen is able to trust the identity of the service provider much as the service provider trusts the identity of the citizen (Fromm, Interview). This is called 'mutual authentication'. The original policy intention was that a service provider would need a different authorisation for each application. For example, if a company had two different websites for two different online software products, they would need an authorisation, and therefore a technical certification, for each. For e-government applications, authorisations may be granted at a variety of levels: application, agency, or for an entire state. For example, there is a portal for a variety of civil services offered by the state of Bavaria, and a single application for the city of Köln to notify the city if you change your address (DE-G002, Interview). The legal and political structure of the individual states help determine if an individual office or region seeks its

own certificate or falls under a larger political entity's certificate (DE-G002, Interview).

The lack of a central database for e-IDs is also a notable data protection characteristic. In the federated identity model, with identity providers and relying parties, the German model relies on a single identity provider (the government) that acts only in an 'offline' mode. The link between the credential and the issuer is severed by design – the system's architecture makes it impossible for the government to track or know of the online activities of cardholders (Bender, et al., 2010, p. 14). This is a form of unlinkability: identity provider blindness to the credential's use. A government scientist stated:

> "We have no centralised servers.... We have no possibility to do any observations on the whole system, so as a government we don't know what happens. That is by design." (DE-G001, Interview)

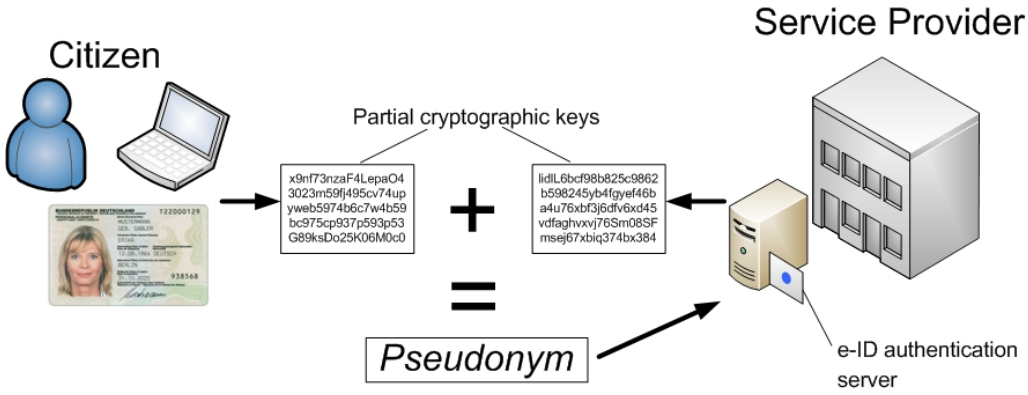
The German population can be largely disambiguated by the combination of first and last name, birthdate and place of birth (Kubicek, Interview; Möller, Interview). In addition to informational self-determination (see below), the birthdate selective disclosure feature was added to frustrate profiling of citizens (Möller, Interview) – by withholding a birthdate, it becomes harder to be sure you are gathering information about a unique individual. Jan Möller (Interview) explained:

> "If you want to make sure that you have the right person basically you'll try to get name … birthdate and place of birth. So this together gives you a very good probability actually to have one certain person … people are kind of collecting these birthdates to have this uniqueness of a certain dataset. And because [of this] we wanted to have the opportunity to let the other side know that somebody is over/under a certain age but not to have this uniqueness."

Pseudonymity function

The pseudonym generator on the e-ID contains 'half' of the necessary maths to create pseudonyms. The other half is contained in each service provider's technical certificate described above. When a cardholder communicates with a service provider who's been approved to access the card's pseudonym function, the two halves come together and produce a pseudonym. This means that each pseudonym is 'card- and service provider-specific' – different service provider certificates will always produce different pseudonyms, and different cards will always produce different pseudonyms.

Figure 6.5 The e-ID pseudonym generation process



Thereby, in terms of these pseudonymous identifiers, the result is unlinkability. That is to say, in the absence of other linkable attributes, service providers should not be able to link a cardholder's online activity via his or her credentials. However, though there is an intention for each service provider to obtain a different authorisation, this has not happened with regard to government agencies. Depending on how e-government services are delivered by a political entity, authorisations are granted for individual offices, agencies, cities and entire states. Since the pseudonyms are card- and service provider-specific, a single pseudonym is produced by one certificate, and therefore could be linked across any applications that fall under that certificate. For

example, if all e-government services for the state of Bavaria fall under a single, state-level authorisation, then all services that rely on the certificate for interactions with the e-ID would see the same pseudonym. By law, the e-ID has a 10-year validity, meaning that no pseudonym generated by the card can be used for more than 10 years.

Four key use cases were envisioned for the pseudonym generator (DE-G002, Interview):

- pseudonymous login
- unique pseudonym to assist identification
- pseudonym without personal data
- pseudonym with verified attributes

In the first case of pseudonymous login, a cardholder would register at a service provider upon an initial visit providing his name and other personal details. At the same time, a pseudonym is produced and included among the other personal data. The cardholder could subsequently log in with the pseudonym rather than a more linkable username or email address. The second use case envisioned was to add a pseudonym to a user account in order to disaggregate her better. Many Germans share similar names (DE-G001, Interview; Möller, Interview), and the use of a pseudonym in conjunction with a common name would uniquely identify the cardholder within a service provider's records without having to obtain more personal data, such as place of birth (DE-G001, Interview). The third case is the use of a pseudonym with no additional personal data. Examples given include an internet service that does not require personal data to create an account, and the use of pre-paid services, where the provider needs to know that money has been submitted but does not need other information except that when a person returns to pay again, it is the same person (DE-G002, Interview). The fourth use case is the transmission of the cardholder's attributes – place of birth, residence, age, etc. – without a name. One possible example cited is that of a library that can only download certain digital materials to people living within a certain area

(Möller, Interview). Another example is registering to volunteer as an election assistant in a local election where the requirement is that you are from that locality (Fromm, Interview). In both examples, the pseudonym could be associated with the verified residence, confirming the bearer's eligibility without disclosing her or his identity, and then affiliated with a local identifier for the bearer to continue the interaction with. The third and fourth use cases are examples of unlinkability as other linkable information about the person is not being passed to the relying party. The first case yields unlinkability with respect to credential usage subsequent to initial enrolment.

Policy Summary

The German e-ID was rolled out to citizens in late 2010. As both the old and new identity card have 10 year validities, by 2020, all German citizens 16 or older will possess an electronic ID card (or a passport). The e-ID serves the same function as the original paper ID – an official identity document for visual inspections – but has additional features by virtue of its electronic components. The e-ID is a contactless card with chip that contains all of the data displayed on the card's face, plus an option for digital fingerprints. The digital face and fingerprint biometric data can only be accessed in a face-to-face interaction by officials who possess authorised readers; they can never be sent from the card through the internet.

The e-ID can electronically authenticate the bearer online. For a service provider to access the data on the card, it must have received a legal authorisation which is then used to obtain a technical certificate. It was originally intended that each service provider must obtain a different authorisation for each application, but this is being applied only to commercial organisations. Government agencies sometimes get authorisations that cover multiple applications, or an entire state's e-government resources. During the authorisation application process, the Federal Office of Administration ensures

that only the minimum amount of data required will be accessible. In addition to sending identity data, the card is capable of indicating if the bearer is born before or after a certain date without disclosing the actual birthdate. It can indicate that the bearer resides within areas of declining size (state, region, municipality, etc.) without disclosing the actual residence. The card can also produce pseudonyms for use in online interactions. E-IDs are shipped with the authentication function switched off and citizens are given the option to turn it on when they obtain their card from their municipal registration office. 72% of cardholders have left this function off (Bundesverwaltungsamt, 2013).

Service provider authorisation certificates contain cryptography that, in combination with cryptography on each e-ID, produces pseudonyms. Each card produces different pseudonyms, as does each service provider certificate. In the case of an umbrella certificate for a state, region, or specific agency, the same pseudonym would be linkable across multiple uses. In the absence of other linkable data, two different pseudonyms are unlinkable.

The overall e-ID infrastructure has no centralised servers, and the government cannot track citizen usage of the card. However, a number of companies are offering 'proxy' e-ID services. Deploying and managing e-ID authentication services at a service provider requires some cost and expertise. Third parties are offering that service to organizations who wish to access e-ID card data but are not prepared to build and maintain the local infrastructure to do so. Theoretically, these proxies could link certain activities of citizens, though it would be illegal and likely violate commercial contracts with the service providers (Kubicek, Interview).

The technical guidelines that detail the pseudonymity function (Federal Office for Information Security, 2011), the cryptographic functions on the e-IDs, the e-ID system architecture and its specific lack of centralised servers, and

supporting policies all together constitute the German policy of unlinkability. The next section explores themes within the empirical data that further explain the genesis and context of the policy.

Themes

Within the case data are a number of themes that are repeated by different respondents, or are otherwise salient because of their relationship to the literature or research questions. This section examines the key themes emerging from the case which are relevant for explaining the process through which unlinkability is emerging in German public policy. See the *Analysis* sub-heading in Chapter 3 for a complete explanation of the thematic analysis techniques employed. The headings of the sections are derived from the thematic coding and analysis of the data.

The first section below discusses the right to informational self-determination, a fundamental principle of German data protection and privacy regimes. In relation to the thematic categories generated during analysis of the empirical data, this right emerged from the Policy category. Next the prevailing privacy 'mindset' in Germany is analysed. This emerged from the Cultural category. The section following discusses the greater protection of validated personal data on the e-ID versus data obtain through other means. This emerged from the Policy analytic category. The e-ID's relationship to the electronic passport is then analysed. This theme emerged from both the Policy and Architecture & Standards categories. The following section analyses the commercial dimension of e-ID policy generally and privacy specifically. This theme emerged from the Business analytic category. Technical versus social methods of privacy enforcement are analysed, followed by a discussion of the marketing of the e-ID. These themes emerged from the Policy and Business categories, respectively. Finally, the various policy actors and usability considerations are reviewed. These themes emerged from the Players and Usability categories.

Informational self-determination

A recurrent theme within the case data is the *right to informational self-determination*. This right is the "legal anchor for data protection in the German constitution," (Hornung and Schnabel, 2009, p. 84). This section details its history and relationship to the data protection and privacy choices made in the development of the e-ID.

In 1982, the German federal parliament passed an Act requiring a general population census to take place the following year. The Act triggered a large, contentious debate and was challenged in the Bundesverfassungsgericht, the German Constitutional Court. In its December 1983 decision, the court found the Act unconstitutional for its lack of procedural and organisational safeguards of citizens' personal data (Hornung and Schnabel, 2009, p. 85; Poullet, 2009, p. 215). In its reasoning, the court derived a right to informational self-determination from the German constitution's rights to dignity and the development of one's personality (Cannataci, 2008; Hornung and Schnabel, 2009; Poullet, 2009; Rouvroy and Poullet, 2009). This right protected "… the authority of the individual to decide himself [*sic*], on the basis of the idea of self-determination, when and within what limits information about his private life should be communicated to others" (Bundesverfassungsgericht [BVerfG] cited by Rouvroy and Poullet, 2009, p. 45).

The first article of the German constitution states:

> "The dignity of man shall be inviolable. To respect and protect it shall be the duty of all states and authorities." (Grundgesetz, cited by Rouvroy and Poullet, 2009, p. 53)

The second article states:

> "Everybody shall have the right to the free development of his [*sic*] personality insofar he does not violate the rights of others or offend

> against the constitutional order or the moral order." (Grundgesetz, cited by Rouvroy and Poullet, 2009, p. 54)

An earlier decision of the court had deemed that the depth of questioning a census would pose and its potential to draw far-reaching inferences about the populace was constitutionally problematic:

> ''It would be contradicting the constitutional guarantee of human dignity for the government to claim the right to compulsorily register and index an individual's complete personality even in the anonymity provided by a statistical census, since the individual would be treated as an object accessible to an inventory in every way.'' (BVerfG cited by Hornung and Schnabel, 2009, p. 87)

This reasoning was used in the 1983 decision and linked with the new right of informational self-determination (Hornung and Schnabel, 2009, p. 87). The census Act had "no clear definition of the objectives, [and] no clear or transparent procedure for following or identifying inaccurate information regarding German citizens. These deficiencies constituted an attack on human dignity and the proper development of the person" (Poullet, 2009, p. 215).

Articles 1.1 and 2.1 of the German constitution form the "general right of personality," guaranteeing each individual the chance to fully develop her or his personality (Cannataci, 2008, p. 5; Hornung and Schnabel, 2009, p. 86). Cannataci (2008, p. 5) wrote:

> "It provides protection to valuable aspects/qualities/attributes … of the human personality … not protected elsewhere … and forms a final barrier against the erosion/penetration of privacy in the personal domain."

The personality right is tied to the capacity for self-determination. The Constitutional Court stated:

> "The value and dignity of the person based on free self-determination as a member of a free society is the focal point of the order established by the [Constitution]. The general personality right … serves to protect these values.…" (BVerfG cited by Poullet, 2009, p. 215).

To facilitate the right to the unhindered development of one's personality, there are number of implementations, or 'sub-rights'. These include the right to one's own image, the right to know one's biological parents, the right to have a sex change, and the right to informational self-determination (Hornung and Schnabel, 2009, p. 86). Hornung and Schnabel (2009, p. 86) wrote:

> "In the German understanding, the right to informational self-determination, as the constitutional anchor for data protection, is a part of the general personality right. It is therefore closely connected to and serves the idea of giving every person the possibility to develop a free and self-determined personality."

The 1983 Constitutional Court believed that information technology had reached a point that was especially challenging to the safeguarding of self-determination. This was due to the capacity for near-instantaneous, automatic processing that could occur with no control by the subject. The court wrote:

> "It is particularly endangered because in reaching decisions one no longer has to rely on manually collected registries and files, but today the technical means of storing individual statements about personal or factual situations of certain or verifiable people with the aid of automatic processing are practically unlimited and can be retrieved in a matter of seconds irrespective of distance. Furthermore, they can be pieced together with other data collection … to add up to a partial or virtually complete personality profile, the persons controlled having no sufficient means of controlling its truth and application." (BVerfG cited by Rouvroy and Poullet, 2009, p. 53).

The right to informational self-determination has two foci. First, providing individuals with the capacities to know about and act upon information about them. Without them, an individual cannot freely plan or decide elements of his life. The court reasoned:

> "If someone cannot predict with sufficient certainty which information about himself in certain areas is known to his social milieu and cannot estimate sufficiently the knowledge of parties to whom communication may be possibly made, he is crucially inhibited in his freedom to plan

> or to decide freely and without being subject to any pressure influence." (BVerfG cited by Rouvroy and Poullet, 2009, p. 53)

Correspondingly, the court believed that citizens must also be aware when information is being collected about them lest they alter their behaviour for fear of being watched:

> "If citizens are unsure whether dissenting behaviour is noticed and information about them is being permanently stored, used and passed on, they will try to avoid dissenting behaviour so as not to attract attention." (Hornung and Schnabel, 2009, p. 85)

The second focus is the protection of democratic society. The court felt that individuals who cannot fully develop their own personalities and determine their own fates cannot fully contribute to democratic processes. Data protection rules thereby preserve the democratic state and are the state's obligation to its citizens. Hornung and Schnabel (2009, p. 86) explained:

> "… data protection is … a precondition for citizens' unbiased participation in the political processes of the democratic constitutional state. The democratic constitutional state relies to a great extent on the participation of all citizens and its legitimacy is based on respecting each person's individual liberty … the right to informational self-determination is not only granted for the sake of the individual, but also in the interest of the public, to guarantee a free and democratic communication order." (Hornung and Schnabel, 2009, p. 86)

Rouvroy and Poullet (2009, p. 55) concurred:

> "Maintaining and fostering private *and* public expression of individuals' thoughts, preferences, opinions and behaviours is among the obligations of the State in democratic societies."

Specifically, the court felt that conditions that could cause citizens to abandon their fundamental rights because of fear and risk would harm the "common good" of society (BVerfG cited by Rouvroy and Poullet, 2009, p. 47).

The 1983 Constitutional Court decision also prohibited the introduction of a unique personal identifier for any German citizen (Hornung and Schnabel, 2009, p. 87). The court saw such identifiers as "an enabling step to collecting and compiling all personal data related to an individual," and as such, would violate that individual's dignity (Hornung and Schnabel, 2009, p. 87). Furthermore, the court decided that the state could not be considered to be a single entity with regard to the collection and use of personal data – an "informational separation of powers" was required (Hornung and Schnabel, 2009, p. 87). This concept was first introduced in the German state of Hesse thirteen years prior in the world's first data protection act (Burkert, 2012, p. 101; Noack and Kubicek, 2010, p. 95). The separation of powers is based on two key data protection principles: purpose specification and proportionality. This first principle mandates that the purpose for which data is collected and processed must be stated at the time of collection, and that subsequent processing does not deviate from the stated purpose (Burkert, 2012, p. 101; Hornung and Schnabel, 2009, p. 87). The second requires that methods used in relation to personal data collection and processing are suitable and appropriate, and not more intrusive than necessary. English judge Lord Diplock (cited by Kuner, 2008, p. 2) saw proportionality as:

> "In plain English, it means 'You must not use a steam hammer to crack a nut, if a nutcracker would do.'"

These two principles in combination led the court to conclude that the state as a whole cannot be considered a single data processor, and that data transfers from one state entity to another must be legally justified (Hornung and Schnabel, 2009, p. 87; DeSimone, 2010, p. 297). Also, the two principles yield the principle of data minimisation – "there must never be more data collected than absolutely necessary for a given purpose" (Hornung and Schnabel, 2009, p. 87; see also Zwingelberg, 2011, pp. 151-152; Kuner, 2008, p. 3). In addition to German law, proportionality, purpose limitation and data minimisation can

be found in European data protection law, to which Germany is subject (Kuner, 2008; Zwingelberg, 2011, p. 153).

The rights and principles above – informational self-determination, purpose specification, proportionality and data minimisation – are at the heart of the data protection and privacy principles at work within the e-ID. The mutual authentication of citizen and service provider, visibly proven through the AusweisApp, notifies a citizen of the identity of a data collector/processor, reflecting a principle of transparency; an imperative for informational self-determination. Mutual authentication is also hoped to inspire trust in the e-ID system, which is conducive to system adoption (Möller, Interview; Rahaman and Sasse, 2010, p. 607). Contained within the service provider certificate are the name and contact details of the provider's responsible data protection authority, giving the user an avenue to question or report the provider's activities. This serves informational self-determination as it gives citizens a route to take action against data processors. One researcher stated:

> "… from a consumer point of view you get to see the certificate, so you actually know who your provider is, actually who is his data protection authority … so you can claim if anything goes wrong you know [whom to talk to], and you see which bits of the data they collect.…" (Hornung, Interview)

Also, citizen reporting is the first step in the prosecution of a malefactor. The BVA does not proactively police individual service providers, but does become involved if a data protection authority requests it (DE-G002, Interview). An author of the e-ID law said:

> "… basically we use the citizen as an indicator that something is wrong … they can just press a button then to say that's something not okay and then it goes either to the privacy officer of the company or the private commissioners [next], and finally if [multiple reports are received] or something is going wrong, they can approach the BVA and say 'there's something wrong, please cut off or take back the [service provider authorisation].'" (Möller, Interview)

In a transaction conducted through the AusweisApp, all of the data requested by the service provider is listed, aiding the goal of transparency. The citizen is given the opportunity to deselect individual data fields to be sent to the service provider. However, a procedural safeguard exists to ensure that the data fields being requested are in fact the minimum required, proportional to the application's need: the BVA application process. And, a service provider is not required to complete a transaction if all of the requested fields are not sent. Despite this, the user is still given the opportunity to deselect fields, though it may cause the transaction to fail. In consideration of the friction that privacy introduces, discussed in Chapter 4, the failure of the transaction can be construed as the maximum friction possible. The balance between the government's desire to facilitate trustworthy authentications and its requirement to safeguard informational self-determination is, in this case, clearly tilted in one's favour. A scientist recalled:

> "Some people said, 'Okay, don't make it optional, you know, show the data which is read from the German e-ID and sent to the service provider and just write Do you agree?, then type in the PIN.' … But the other half of them said 'No but we want that the citizen sees which data is sent and has a choice.' And now I have the choice, but to be honest, if I want this service, I don't have a choice, but still *this* solution … is putting the expression on having a choice. Until the last moment the citizen has a choice to say 'No.'" (Fromm, Interview).

The e-ID's selective disclosure feature serves the principle of minimal disclosure. For those transactions where age or age range is needed, birthdate can be withheld. For those where proof of regional residence is required, full address can be withheld. Minimal disclosure is also enforced by the BVA application procedures. State officials act as guardians of the 'sovereign' data on the e-ID, ensuring that commercial and government organisations only gain access to the data truly necessary (in their view) to accomplish a transaction.

This is supported through technical means via the service provider certificates, which can only be obtained after a successful application to the BVA.

The pseudonym generator serves a number of goals. The first is minimum disclosure. For those transactions where a service provider needs to know that the same person is returning and nothing else, or that a citizen has particular attributes (e.g., age or region) but does not need identity information, pseudonyms support this. The second goal is informational self-determination, by providing the means to separate the spheres of one's online activities, controlling the dissemination of information about one's digital life. The right to the full development of one's personality is assisted by giving citizens the ability to control which parts of themselves they wish to reveal. A staff member of the ULD explained:

> "… the citizen must be able to intervene and decide if information should be linkable or not. Another aspect would be that it also gives them the freedom to actually act or live just certain aspects of their personality … the big risk is that you have all information dumped into one database, and the risk is also here that the citizen is reduced to this information.… So, it's a personal freedom to decide which aspect of your personality you want to reveal and you want to use, and so it is quite important to offer them to open that possibility to them." (ULD, Interview)

This is further supported by the 'sectoral' nature of service provider certificates, in line with the Constitutional Court's finding that the state cannot act as a single data processor.

The card's 10-year validity supports the Constitutional Court's forbidding of long-lived general identifiers. This also ensures that pseudonyms – since they are card- and service provider-specific – become invalid within 10 years. The voluntary nature of the online authentication function serves informational determination by giving users the ability to decline its use. This is also true of the voluntary inclusion of fingerprints.

Privacy mindset

A number of respondents cited a 'privacy mindset' as part of the policy universe of the e-ID, described variously as:

- a "philosophy" (Fromm, Interview)
- a "mindset" (DE-G003, Interview; ULD, Interview)
- "culture" (DE-G003, Interview; Möller, Interview; ULD Interview)
- a "value" (Fromm, Interview; DE-G003, Interview)

This mindset was partly attributed to German history: the use of identification information by the Nazi and East German regimes to control, hunt and kill its citizens (DE-G002, Interview; Fromm, Interview; Kubicek, Interview). The 1983 Constitutional Court decision forbidding unique personal identifiers draws on this history (Noack and Kubicek, 2010, p. 88; Hornung, Interview; Kubicek, Interview). Noack and Kubicek (2010, p. 88) explained:

> "In 1938, the National Socialist Regime (Third Reich) introduced an ID card with fingerprints, which was mandatory only for conscripts and Jewish citizens. 1939, with the beginning of the Second World War, it became mandatory for every citizen and inhabitants of the occupied territories. Jewish citizens were also assigned with numbers, which were used for their deportation and administration in concentration camps… This specific historical context has influenced the debate about … [the e-ID] in the last 10 years just as it did the earlier debate about a unique personal identifying number."

The extent of that influence is debatable, however. Gerrit Hornung (Interview) observed:

> "… we've had like two historic experiences, and one is only twenty years ago with the Stasi [East German police], and obviously that sort of influences … political discussions, those experiences. I am not sure … whether it goes a lot further than having this historical background as a general base for the discussions, because I don't see a direct connection from the having fingerprints on the Third Reich identity cards … and having it now."

Nonetheless, the respondents believe that privacy is a valued, oft-considered concept in Germany (DE-G002, Interview; DE-G003, Interview; ULD, Interview). Gerrit Hornung (Interview) noted:

> "… the data protection issues and privacy issues in Germany are strongly debated always in every … new security application, new collection of data.…"

Some saw the choice to include the pseudonymity feature of the e-ID as driven not by "a specific service or application … it was more, let's say … a general approach following … a common mindset" (DE-G003, Interview). Given the e-ID's other privacy functions, the pseudonym generator was "logical" to include (ULD, Interview). A data protection officer said:

> "I think putting the pseudonymity function is a must-have concept when once you already have these other anonymous authentication methods or age or the municipality you live in, and basically putting the pseudonym in as another function in this privacy area … it is just more or less logical." (ULD, Interview)

Pseudonymity requirements exist elsewhere in German law. The *Telemediengesetz* (Telemedia Act), which applies to telecommunications services, includes a provision requiring service companies to enable users to be able to use and pay for services pseudonymously (Telemedia Act, 2007, Sec. 13(6)). The companies are forbidden from attempting to identify a pseudonymous user through combining other data it possesses (Telemedia Act, 2007, Sec. 13(4)). These provisions pre-dated the e-ID and contributed to the mindset for pseudonymity (ULD, Interview).

There is awareness among a few of the respondents that the German privacy culture is not embraced by other European countries. Some see the degree of data minimisation and the administrative processes of the BVA as "typically German" (Fromm, Interview; DE-G002, Interview; also N003, Interview). Jan Möller noted:

> "… privacy and self-determination, it's a big issue in Germany.… [W]ithin Europe it's totally different … what people in these societies consider … is within this privacy sphere and what is not … Germany probably has a … higher wish for a bigger private area." (Möller, Interview)

One respondent believed that there was a strong trust in Germany for the original paper ID that could transfer to the e-ID: "… it has established itself as a trustworthy document – no one in Germany doubts this document" (Fromm, Interview). Further, this trust led to a preference for the existence of a state-issued 'sovereign' identity rather than only having commercial ones available. Jens Fromm (Interview) explained:

> "I have the strong feeling that I don't want to be dependent on commercial identification.… I think that it is good that we have this, but I don't want to depend only commercial identities like a PayPal account or a Google ID, a Microsoft passport approach. It is great that we have all these solutions and companies are offering this… but in some cases, in some situations, I am strongly convinced that it's good that we have a sovereign state-given identity. For example, to open up a bank account, to have governmental services, to use in any kind of situations, I think I don't want to involve any kind of other companies."

Stronger protections for validated data

The case data reflects a belief that the personal data contained on the card – sometimes referred to as 'sovereign' data by respondents – is deserving of greater protection than publically or commercially available information about citizens, or than data that they volunteer themselves (Fromm, Interview; Möller, Interview; ULD, Interview). Policy discourse during the genesis of the e-ID reflected this dichotomy. A scientist active in the e-ID policy community noted:

> "... what was very interesting the last five years, listening to data commissioners, listening to left wing politicians, right wing politicians, whatsoever … you know people are active on Facebook, they are writing emails so basically, a postal card through the 'net … when you are buying products sometimes the cashiers ask for the postal code and

> they are just giving it, they have [loyalty] cards, they have all this kind of stuff … as soon as we talk about the German identity card, each data field is discussed and protected like it would be you know, in England, the Queen or something." (Fromm, Interview)

In part, the impulse to protect it comes from a belief that validated data is qualitatively different because it can be trusted. Jan Möller stated:

> "So it's just a different quality if you have proven from the card or you have just any information on the web; it makes it different. It needs different protection… You can trust it, trust is the currency." (Möller, Interview)

However, it's also been suggested that the focus on the card data derives from the capability to influence it; that protection of the data falls within the remit of the responsible authorities, and so they are exerting their prerogative (Kubicek, Interview). To support increased protection of the official data on the e-ID, it was made illegal to store proof that authentication data originated from the card; partly to eliminate the possibility of a black market in authenticated official data. Jan Möller explained:

> "… they can't use any technical information deriving from this process… they are not allowed to store that stuff, so they cannot prove that actually this authentication with this data took place … we didn't want to have a new kind of currency in the address market like original, national ID data or something like that." (Möller, Interview)

This means that the identity data on the card is not 'signed' when it is transmitted – there is no cryptographic proof that the data originated from the card. However, one researcher has commented that this compromises security:

> "This means that if the [cryptography] is compromised, an attacker can create a card that can send arbitrary data that will be accepted by the server at face value. As a consequence, the attacker can impersonate an arbitrary person." (Hoepman, 2012)

Relationship to e-passport

The e-ID is very closely related to the e-passport. It largely mirrors the e-passport technical infrastructure (DE-G001, Interview; Margraf, Interview). When the Federal Office of Information Security (BSI) was developing the e-passport system, it also had in mind a future e-ID infrastructure. A government computer scientist recalled:

> "… when we started designing the protocols for the e-passport we already had also an identity card in mind. So when we planned for the protocols we planned it in a way we could also base an identity card on those protocols." (DE-G001, Interview)

The e-ID's mutual authentication feature, which serves the goal of informational self-determination (discussed above), was created for the e-passport. In that prior implementation, instead of service providers authenticating themselves to the card, it was border agents with authorised terminals (Margraf, Interview; DE-G001, Interview). During the policy development of the e-ID, there was dissent regarding the mirroring of mandatory biometrics on the e-passport. Marit Hansen of the ULD said:

> "… the Minister of the Interior, Schäuble, he really wanted to press people that they should give their fingerprints like with the e-passport. So in 2006, they issued this initiative, they seem to want to copy everything with the e-passport, and there was many objections from the data protection authorities because of centralisation of the database…" (ULD, Interview)

Both the e-passport and the e-ID fall under the remit of the Ministry of Interior. Gerrit Hornung, a legal scholar of the e-ID, believed that the terrorist attacks of September 11, 2001, played a role in the discourse of both the e-passport and e-ID's inclusion of biometrics:

> "… after September 11, people in Europe started to think about having this biometric passport… and so the German biometric passport [was deployed] in 2007 … and so when people started to implement that project I think there were parallel thoughts on having biometric data on

> the identity card as well…." (Hornung, Interview; see also Noack and Kubicek, 2010, p. 91)

After a privacy debate within the Parliament (Bundestag) that also involved the Federal data protection supervisor, the storage of fingerprints on the e-ID was made voluntary (Noack and Kubicek, 2010). There are no applications, travel or otherwise, that can use fingerprints on the e-ID; non-German governments are not reading the fingerprints stored on the card (Hornung, Interview).

There were manufacturing ties between the e-passport and e-ID. T-Systems, an information technology company part of the Deutsche Telekom group, was a key supplier for both e-passports and the e-ID. One respondent explained:

> "T-Systems was the main contractor for the introduction of the new German … electronic passport a few years ago, and through this activity [they] were well placed and that was the reason why then our German Federal Ministry of Interior asked [them] to take over some responsibilities in the introduction of the new *Personalausweis*…." (DE-G003, Interview)

To improve the security of sending passwords across the e-ID's contactless interface, the BSI developed a protocol called Password Authenticated Connection Establishment (PACE). In addition to use with the e-ID, PACE has since been adopted by the International Civil Aviation Organization, the international body responsible for travel document standards (ULD, Interview; DE-G005, Interview). As such, PACE will become part of the security standards for all next-generation electronic passports (Nithyanand, 2009, p. 10).

Commercial influences

Given the policy history of the e-ID, commercial considerations appear after the *Personalausweisgesetz* was passed and do not appear to have contributed greatly to the law's genesis or provisions, though there was some public

support by industry trade bodies for the online authentication and e-signature functions (Hornung, Interview). There is some evidence of commercial influence in the presence of the cardholder's postal code in the card data. The German postal system is private so the post codes are privately assigned and do not follow political boundaries (ULD, Interview). The card contains both the post code and the government-created municipality ID. A scientist stated:

> "… on the old German identity card there was no postal code because it was private, now there is a postal code on the German identity card because the companies wanted it, because it's easier for them…." (Fromm, Interview)

Companies from the card manufacturing and IT security sectors were involved by the BSI while they were developing the e-ID's technical specifications. A security researcher said:

> "The BSI did not create the protocols [from] scratch, but of course they were communicating with the card manufacturers and the technicians of the manufacturers, and all the manufacturers they act … internationally." (DE-G005, Interview)

Commercial and government relying parties were involved during a testing period, though there was a lack of strong commitment from industry generally (Noack and Kubicek, 2010, p. 103). At present, one of the greatest challenges to adoption of the online authentication function is a lack of service providers. The difficulty lies in making the business case to commercial providers to go through the certification process. For large international businesses, it is often not beneficial enough to become certified for a German-only system (DE-G005, Interview). Further, the value of the card to commercial companies is only verified data (Kubicek, Interview). While this can conceivably reduce data entry problems, incorrect shipping addresses, and potentially fraudulent logins, it's so far not a very robust case (DE-G002, Interview). There is not a strong enough reason or cost reduction to cause businesses to alter their

practices – the data volunteered by customers or obtained through other means is sufficient. Herbert Kubicek explained:

> "What would be my motivation as an e-commerce provider to buy expensive middleware, to pay annual fees for all these … if I don't get more information then I get by username or password so far?" (Kubicek, Interview)

Furthermore, the policy intention is for commercial service providers to obtain a separate authorisation for each service they offer online, making the process more financially unattractive. It's also been suggested that the maximum 10-year lifespan of a card-generated pseudonym dissuades businesses from using them. Jens Fromm stated:

> "The biggest problem of the pseudonym function, it's at the same time the biggest advantage of the pseudonym function.… As soon as I lose this card, as soon as this card gets invalid and I get a new identity card, I get a new key on it and I cannot generate the same pseudonym with this service provider. Many companies … wanted to use this number in the beginning as a … permanent unique identifier. So this doesn't work." (Fromm, Interview)

As a result of these various challenges, administrators at the BVA spend more than 50% of their time trying to convince service providers of the value of becoming certified to access data on the e-ID (DE-G002, Interview).

The e-ID has an electronic signature function that is enabled by loading on privately obtained certificates. However, that function is currently dormant in all e-IDs because no companies are selling the e-signature certificates. Contact-based e-signature cards have been sold privately in Germany since the early 2000s. Those vendors do not see a benefit in offering certificates for the e-ID as it could potentially 'cannibalise' their own markets by supplying a product that would compete with their own extant offerings (DE-G003, Interview).

The e-ID is also new and those businesses that might be inclined to use it – German-based businesses, for example – may need time to adopt it. Jens Fromm (Interview) observed:

> "... now we know that obviously we need to give this technology time and we need to give the companies time to offer services, and obviously a big company like Deutsche Bahn, the German train company, or the Tax Ministry, they don't introduce a new technology within three months. They need to go to certification processes, they need to integrate it in their data centres, they need to train people, so these are obviously processes that will take time…."

Technical vs. social methods of privacy enforcement

The privacy functions of the e-ID are accomplished largely through technical means. The card contains mathematical functions that enable selective disclosure of attributes, such as age range or locality. Different functions generate unlinkable pseudonyms when matched with cryptographic data contained in service provider certificates. The data protection model is broadly underpinned by cryptography: cards will only communicate in the presence of appropriate cryptographic certificates, data communications are encrypted, the card's revocation method is a complex cryptographic system. In the case of bad actors, where a service provider is suspected of mishandling personal data, the BVA can order certificate authorities to invalidate the offender's certificate, technically preventing data from flowing.

The choice to eschew centralised databases in the overall architecture reinforces the strong privacy impulse to prevent the state from knowing about its citizens' online activity. The e-ID system, by design, disallows the state from tracking cardholders online. During the development of the e-ID policy, stakeholders reviewed the Austrian e-ID system which also rejected long-lived identifiers. However, the system relied on servers that could link citizen activities and so the architecture had a limited influence on German technical choices (Fromm, Interview). Similarly, the lack of centralised databases of

biometric information held on e-ID cards supports the rejection of an informationally intrusive state. Further, the biometrics can only be accessed in a face-to-face interaction – the architecture prevents the data from any other form of access. This layer of technical security further prevents the accumulation of biometric databases of the citizenry.

The technology that underpins the e-ID's security and privacy features are largely derived of the German e-passport design, allowing the e-ID to easily inherit those features (Möller, Interview; Noack and Kubicek, 2010, pp. 108-109). The pseudonym generator and selective disclosure features are unique to the card, and represent an intention to anchor privacy intentions in a technical model. Jan Möller explained:

> "… where we had the real trust anchors of the whole system, we tried to secure them in a technical way because this is not dependent on how far you can actually enforce law. But of course you cannot do everything in a technical way. So sometimes we had to look for protections which were in a legal way then.… So it's a mixture of both, but … the real important bits you want to have in a technical secure way or you want to have technical mechanisms to make sure that they are enforced." (Möller, Interview)

There are a number of non-technical methods of privacy enforcement. Firstly is the *Personalausweisgesetz* itself; it requires data minimisation principles to be applied to service providers who wish to access the card. It also forbids anyone from asking a citizen to surrender her or his e-ID (Möller, Interview). The BVA's application procedure is policy-driven. The 1983 Constitutional Court decision that derived a right of informational self-determination is the key influence driving privacy and data protection for the e-ID, in addition to the general German data protection law, itself a transposition of the European Union Data Protection Directive. Privacy sensitivity around biometrics is supported by policies requiring that the federal printer must delete any facial photographs or fingerprints it receives after producing a card (DE-G001,

Interview). Contracts are used by service providers to control the behaviour of e-ID service proxies, who are also subject to data protection law. Service providers are prohibited by law from recording cryptographic provenance of authentication data so data cannot be proven to have originated from the e-ID (Möller, Interview).

Marketing

Weak 'marketing' was cited as a key obstacle to broad adoption of the online authentication function (DE-G002, Interview; Fromm, Interview; ULD, Interview). Citizens were not effectively made aware of the online authentication – and hence its pseudonymity capabilities – or the value of it. Relatedly, municipal registration office workers were not trained well enough to discuss or support the authentication function (DE-G002, Interview; Fromm, Interview). There are approximately 6,000 municipal offices; an estimated 20,000 people needed to be trained in those offices to produce and distribute the e-IDs (Fromm, Interview). As the citizen's main point of contact for obtaining an e-ID is her or his local municipal registration office, the insufficient training led to citizens receiving inadequate and inconsistent details about the authentication function and where it might be used. A government official stated:

> "When you get your card you can decide, and roundabout only 30% … decide to [turn on the authentication function].… And the first contact you have with the card [is] your local municipality office, and our way is to convince [those employees] because they have the first contact to the citizens. [It's] a great problem because they are not marketing [professionals]." (DE-G002, Interview)

> "Why should citizens use the identity function, are they aware of these identity functions? About 65% of the citizens are opting out the function because they just don't know why they should use it, why they should opt in … if any other countries are thinking about this system, education, marketing is crucial." (Fromm, Interview)

Part of the BVA's strategy to encourage adoption of the authentication function is to convince more public agencies and services to use the e-ID as part of their e-government strategy so as to illustrate its value to the citizen:

> "… the best way is it to show that the e-government business is working because then you can say, 'It's okay for you [to turn the authentication function] on and not off because in our own community it works.'" (DE-G002, Interview).

The issue of marketing illustrates the product nature of the e-ID. As a material trace of a citizen's official identity, the e-ID must be treated akin to other products and services, and must compete for space in the market for people's attention. One official explained:

> "… this chip and this card is a product and nothing else. It's an official product from Germany… Other persons, offices, they say, 'Only it's a legal decision to make this card,' final point, nothing else. For me it's a product and you have to [do] marketing… you have to go [to] the users, you have to go to the business cases and you have to decide what you want." (DE-G002, Interview)

As noted above, BVA officials responsible for managing the e-ID spend more than 50% of their time attempting to convince both governmental and commercial organizations to adopt the e-ID (DE-G002, Interview). They put on, in essence, a road show:

> "… we initiate conferences, we go to the states, we go to the cities, we talk to them and inform them about the possibilities and the functions that they could use just so that they get an idea of what they can benefit from." (DE-G002, Interview)

To help agencies and private organisations successfully apply for a certificate, the BVA consults with them iteratively to find the minimum set of data needed for an application. The official notes:

> "… they have an idea and they initiate a project and say, 'We want to do this and that' and then we consult people and say, 'Okay, what do you really need?' and this is really a process.… It's not in the legal

system but we do it because we have learned that the other way is not good." (DE-G002, Interview).

When the federal government first began to discuss the e-ID in public, they, too, put on a road show to make the case to the citizenry of its value and security characteristics. The Ministry took branding and recognisability into consideration, adding a logo to the e-ID to help bearers know where they could use their card.

Figure 6.6 The e-ID logo

Source: Federal Office for Information Security, n.d.

Jan Möller (Interview) noted that the two halves depicted in the logo symbolise the uniting of the physical world and the electronic one.

Policy actors

The key actor in the creation of the e-ID was the Ministry of Interior. The earliest appearance of a policy intention to change the laminated paper national identity card to the *neue Personalausweis* began and ended with the Ministry. Its influence is evident through the legislative process that created the e-ID law, the ground preparation of the citizenry, and through its sub-agencies the development of the card's privacy architecture and certification system to

authorise service providers' access to citizen data. The Ministry essentially wrote the e-ID law in consultation with the German parliament (Möller, Interview). The technical guidelines, architectures and policies that underpin the *Personalausweisgesetz* were largely inherited from the e-passport system, which the Ministry also administers (DE-G001, Interview; DE-G005, Interview; Margraf, Interview). The section of the law requiring service providers to be authorised to access data on the card gave no details for implementation, and so was interpreted and developed by the Federal Office of Administration (BVA), an agency within the Ministry. They convened a working group made of state and federal data protection officers, the BSI, representatives of private companies, and government administrators, with observers from the Ministry. As regards the e-ID's privacy functions – pseudonymity, mutual authentication and selective disclosure – they were added to the design by Jan Möller who had been hired by the Ministry specifically to be one of the authors of the e-ID law. Mr. Möller is the chief figure inside the Ministry responsible for the e-ID's privacy features. He recalled:

> "we had the basic idea [of the privacy functions] from the beginning … this was my idea as far as I was involved, that we wanted to build a function people want to use because they can trust it. So I wanted to build something what I also myself want to use because it takes care about my rights and my self-determination." (Möller, Interview)

Herbert Kubicek (Interview) remarked on the trust placed in Mr. Möller:

> "[The Ministry] hired Möller to take care of the privacy issues. And my impression is that they didn't really care what he proposed because they believed in him, because the ULD is the most critical of all sixteen privacy state offices. So if they agree with something, you can be safe that there will be no discussion following."

The federal police, also a sub-agency of the Ministry of Interior played a role as well. When it was decided that the e-ID would conform to ID-2, the size of banking cards and other European e-IDs, the police were insistent that the size

of the photograph on the original ID not be reduced so as not to make visual identifications more difficult (Noack and Kubicek, 2010, p. 96; Fromm, Interview; DE-G001, Interview; ULD, Interview). This, in turn, influenced the technology of the card: more space for the photograph left less 'real estate' for an electronic chip. This eliminated the possibility for a contact-based chip, forcing the use of a contactless chip, which, due to its capacity for more data storage, opened up the possibility for more functionality (Noack and Kubicek, 2010, p. 96).

Federal and state-level data protection authorities were also key players in the e-ID's development. At the federal level, the data protection supervisor was vocally opposed to the mandatory inclusion of fingerprints or a national centralised e-ID database (Hornung, Interview, ULD, Interview). The state data protection authorities provided commentary during the policy development of the e-ID. In particular, the ULD was involved due to its expertise in electronic identity having participated in the pan-European projects, Future of Identity in the Information Society (FIDIS) and Privacy and Identity Management for Europe (PRIME). The ULD's deputy commissioner, Marit Hansen, has published numerous identity management and privacy-related papers and articles, and was Jan Möller's manager when he was at the ULD (Möller, Interview; ULD, Interview). In early January 2010, data protection authorities were asked to interpret the e-ID law's requirement that service providers only request the information necessary to perform their duties. The ULD responded with a set of use cases to illustrate the 'principle of necessity' and later published a paper on their findings (ULD, Interview; Zwingelberg, 2011). State-level data protection authorities play an on-going role in enforcement: if they suspect that a service provider authorised to query the e-ID is mishandling personal data, they can notify the BVA who can then cut off the provider's access (Möller, Interview).

The approximately 6,000 municipalities played a role in the e-ID's development and on-going deployment. Constitutionally, the municipalities are responsible for citizen registration (ULD, Interview). As discussed above, the municipalities are the first port of call for citizens wishing to obtain an e-ID. The municipalities begin the process, take new photographs, transmit the data to the federal printer, and then distribute the e-ID upon its delivery from the printer. The municipal offices are the closest source of information about the e-ID, and as such factor greatly in citizen awareness of the e-ID's functions. The difficulty in training and convincing the approximately 20,000 involved municipal workers of the benefits of the e-ID is cited as a reason that less than 1/3 of the cards in circulation have its online authentication function turned on (DE-G002, Interview; Fromm, Interview). The cost of the e-ID – approximately €29 – is nearly three times the price of the original paper identity card (Fromm, Interview). This is largely due to the increased administrative and equipment costs borne by the municipalities (Fromm, Interview; Kubicek, Interview). This increased price caused the Ministry of Interior to consider adding features to the card, such as online authentication, to make the card more valuable to citizens. Jan Möller (Interview) explained:

> "… if you have the chip already you can use it for additional value and so kind of this e-ID function was born as…well we have to have the chip anyway for biometrics and so on, so we will have a more expensive card of cost and all that but then we also want to have extra value for the citizens of it if we have to make it more expensive.…"

However, Prof. Dr. Herbert Kubicek, a scholar from the University of Bremen who has written on the e-ID, does not believe that the additional features were added to make the card more attractive: "There is no stakeholder for this attraction" (Interview).

Academics, universities and research institutions have played a role in the policy history and technical development of the e-ID. Experts in electronic signature law, a related antecedent to the e-ID, were engaged by the

government from the early 2000s onward (Hornung, Interview). Legal analytical texts have been produced on e-ID liability issues. Prof. Dr. Kubicek shared research on use cases for e-commerce with the Ministry (Kubicek, Interview). The Technical University of Darmstadt performed pilot tests, reported on functional and security weaknesses of the e-ID architecture, and worked with the BSI to develop some of the underlying cryptographic protocols used in the e-ID's privacy functions (DE-G005, Interview). The Fraunhofer Institute, one of Europe's largest research institutions, was a "mediator between government approaches and government philosophies and the industry" during the rollout of the e-ID (Fromm, Interview).

Usability

The usability of the e-ID system is a recurrent theme within the data. Jan Möller mentioned that helping users to manage multiple pseudonymous identities was one of his goals during the policy development of the *Personalausweis*:

> "… from my feeling you have to support the people, they don't wanna care about pseudonyms or not … basically they want to be sure but they don't want to care too much about the security issue or the question 'Where did I use it, what profile is behind this pseudonym or not…?'" (Möller, Interview)

Usability concerns were part of the policy-making process. There was a desire to inform which data was being requested by whom and to give users control – transparency and the ability to intervene. But there was also concern of introducing too many steps into the authentication process. Jan Möller (Interview) remarked:

> "… on the one hand you want to get the information for transparency back; self-determination needs transparency and [a] way to act if something is not the way you want to have it. So we needed to build this into the AusweisApp. But on the other hand, nobody wants to hassle with thousands of steps, so we tried to minimise the number of

> steps to go through. This is basically why [the AusweisApp is] just three steps. The first is you read the information, the second is you decide and choose, and the third is put your PIN in, and this is it."

As previously discussed (see Informational Self-Determination above), users are allowed to de-select data fields requested by the service provider even if doing so would prevent the transaction from completing. This is a design choice in service of informational self-determination – giving users the option to say 'No':

> "… if you use public infrastructure for it, it needs to be transparent and you need to have the opportunity to say No…." (Möller, Interview)

The e-ID was designed as a general identity token for the authenticating on the internet. Ease of use was intentional in that citizens only need to enter a six-digit PIN authenticate, rather than remembering multiple passwords for various websites (DE-G001, Interview; DE-G003, Interview). Ease of use was also a consideration in the design of the revocation system. For a citizen to revoke her e-ID because it is lost or stolen, she must begin the process with a revocation password. The password is a simple word from the dictionary so as to be easy to memorise (DE-G002, Interview).

Though there was some usability testing of the e-ID system, some respondents saw it as insufficient (DE-G003, Interview; Fromm, Interview). Jens Fromm (Interview) believed that privacy and security had to be modulated initially so as not to introduce too much friction, reducing adoption:

> "… we are in the rolling out process and the higher you have the [privacy and security] standards in the beginning the less likely it is that citizens are happy to use this … you need to have a system easy to use."

Fromm also felt that using the e-ID consistently as an authentication token for the internet was unrealistic because of the number of times one would have to physically use the card and the AusweisApp:

> "… there were people who believed that this would be used for any kind of identification, authentication, but you know if you look at the young people today using Facebook and hop on, hop off thirty, forty times a day, I think it's quite obvious that they are not prepared to type in a 6-digit PIN and to place their wallet with the German e-ID on the card reader thirty times a day." (Fromm, Interview)

Among some respondents there was a general belief that usability is critical to adoption (Fromm, Interview; DE-G003, Interview), and that it is "one of the most difficult tasks to achieve" (Fromm, Interview). A respondent from industry noted:

> "… the overall major point for me is of course to find a good balance between necessary security on the one hand and secondly usability acceptance on the citizens' side.…" (DE-G003, Interview)

Jens Fromm remarked on the primacy of usability in identity management:

> "… what we learned is really security is not all. It's really about usability … you can have the most secure system – if it's not used, it doesn't change anything because it's not used … we need to go to a usability level where it's being accepted, then we can raise slowly security and privacy issues. It doesn't really work the other way around." (Fromm, Interview)

Conclusion

This chapter reviewed empirical data gathered on German public policies of unlinkability. It explored the context in which unlinkability is nested: digital credentials for citizens to access e-government and commercial websites. Germany began issuing an e-ID card in 2010 that is capable of authenticating cardholders online. The card is able to send verified identification information, such as a name and address, and attributes such as place of birth and doctoral degree. The card can also produce pseudonyms when paired with a service provider's authorisation certificate which allows the provider to obtain data from the card. In the absence of other linkable information, the pseudonyms created by the card and certificate are unlinkable. This is Germany's policy of

unlinkability. Unlike the US, the German policy is strictly one of technical enforcement, relying on cryptography to create pseudonyms and to separate contexts, and by deliberately avoiding centralised servers in the e-ID system's architecture, which renders the system unobservable by government.

This chapter illustrated how, like in the US, policy initiatives to facilitate online authentication of citizens are linked to e-government activities. Unlike the US, German identity management policies are also linked to e-signature policy. This is due in part to the advanced state of e-signature legislation in Germany and Europe, and to an early, unsuitable use of e-signatures as a form of strong authentication. The German e-ID is, technologically, a direct descendent of the German e-passport, inheriting nearly all of its infrastructure design. The e-ID was deployed to facilitate e-government authentication, to change the size of the national ID to a smaller, more common size, and to generally improve the security of online interactions for citizens.

The e-ID's authorising law, architecture, and policy development were driven by the Ministry of Interior. The privacy features of the e-ID were largely driven by Jan Möller, a lawyer who previously worked for the ULD, a German data protection authority. Mr. Möller included the e-ID's unlinkability features, though it did not appear in the authorising law. Unlinkability and the card's other privacy features – selective disclosure, mutual authentication with service providers, and a requirement to obtain an authorisation to retrieve data from the card – did not rise to the level of legislative debate. The only debate on privacy issues centred on the mandatory inclusion of fingerprints. These were ultimately made optional.

The choice to include unlinkability in the German e-ID was informed by a seminal 1983 Constitutional Court case. This case derived a right to informational self-determination from the German constitution. This right is

"the constitutional anchor for data protection" (Hornung and Schnabel, 2009, p. 86). It requires that people know what data is being shared about them, and that they have the opportunity to refuse to share it. The Constitutional Court also prohibited the use of unique identifiers for citizens, and ruled that the state could not be considered a single data processor. Unlinkability serves these prohibitions by creating a different identifier for each person and separating the context of the use of them. German data protection is more coherent than that of the US due to its omnibus personal data protection law, the Constitutional Court case, vocal data protection authorities, and prior law requiring options for pseudonymity. Culturally, German identity management policy was influenced by a privacy mindset.

Similar to the US, commercial issues influence and hinder German identity management policy. Only 28% of Germans have turned on the online authentication feature of the e-ID, largely due to weak marketing and lack of educating the municipal offices who distribute the cards. Administrators and officials had hoped that many commercial organisations would become certified to access personal data on the card, but numbers have remained low. This is mainly because those organisations are not yet convinced of the value of the official data on the card, and so they are unwilling to spend time and resources on becoming certified.

CHAPTER 7: COMPARISON OF GERMAN AND US POLICIES

Introduction

This chapter compares US and German identity management policies for citizen credentials, focusing on requirements for unlinkability. There are similarities and pronounced differences in the policy history and environments of the two countries, but both require identity management systems for citizen access to e-government to be able to create unlinkable pseudonymous logins. The core influence for this requirement is the principle of data minimisation and proportionality, present in German law and in a set of principles underpinning US privacy policy. The German Federal Data Protection Act requires data minimisation, in line with the European Data Protection Directive. The Act goes further, mandating that "personal data are to be aliased or rendered anonymous as far as possible" (Federal Data Protection Act, 2003, Sec. 3a). These requirements, plus a telecommunications law and a seminal Constitutional Court case are the direct antecedents of German unlinkability policies. The US Privacy Act of 1974 and a non-binding set of Fair Information Practice Principles containing the principle of data minimisation guide American privacy policy. These formal instruments directly inform US unlinkability requirements.

A key finding of this research is that the privacy features of the German e-ID and the proposed US Federal Cloud Credential Exchange are some of the most advanced citizen-facing privacy and data protection policies in their respective countries. They are also a notable appearance of privacy-enhancing technology in national information policy. This chapter compares the countries' formal and informal policies, technical and non-technical implementations, data protection models, key actors, the commercial dimension of implementation, and inherent challenges. These topics form the "gestalt" of unlinkability policy development

(McClure, et al., 1999, p. 314) and allow for a direct comparison of the 'how' and 'why' of these policies in Germany and the US (Heidenheimer, et al., 1990, p. 3). Comparing the two countries in this way creates an elaborated context to understand unlinkability and citizen credentialing generally, as well as in each country particularly.

There is very limited empirical research on American citizen credentialing, its privacy architectures and its risk methodologies (Adjei, 2013; Katzan, 2011a, 2011b; Schwartz, 2011). There is also limited research on the German e-ID data protection model, (Hornung and Roßnagel, 2010; Noack and Kubicek, 2010) and little empirical research of unlinkability policies generally. This thesis addresses those gaps.

The research also identifies a sub-branch of information policy, 'identity management policy.' It includes online citizen credentialing activities, government employee and contractor credentialing, the relationship between government and private actors performing identity management services, risk models and policies relating to e-government access. Identity management here is used in the technical sense discussed in Chapter 4; it is systemic, comprised of data, organisationally-derived and transactional. IDM policy overlaps with 'identity policy,' which includes national identification systems, citizenship, and the relationship between citizens, non-citizens and the state (Davies and Hosein, 2007). IDM policy is influenced by data protection and privacy policies, procurement policies, security policies, e-government activities, and the needs of law enforcement and the military.

Germany and the US are both capitalist, advanced democracies. Both have federal and state governments. They both have national policies in place to protect the privacy of their citizens, although there is wide variation in the scope and manner of this protection. Both countries addressed electronic

identity issues during the first decade of the millennium, and both saw significant growth in the use of e-government in that same period. There are many differences between the two polities as well. Germany's population is approximately 80 million (BBC, 2013), whereas the US is approximately 316 million (U.S. Census Bureau, 2013). This difference in population scale affected policy options. Germany is part of the European Union, and as such some of Germany's laws are directly influenced by it; its sovereignty is not completely its own. The United States is not a member of any supranational or intergovernmental entity that can influence its laws to the same degree.

Significant to this research are differences in data protection regime. Germany has a data protection policy 'layer' – a regime comprised of an omnibus data protection law, a federal data protection commissioner, and data protection authorities in each German state. The US is absent this layer; its data protection laws are sectoral, and there are no data protection authorities or commissioners. Different regulatory agencies, such as the Federal Trade Commission, the Securities and Exchange Commission, and the Financial Industry Regulatory Authority, are responsible for different facets of data protection and privacy in their respective sectors.

Another key point of difference between the two countries is the source of citizen credentials. In Germany, the federal government is issuing credentials directly in the form of a national e-ID card. They manage and pay for the identity supply chain: enrolling citizens and residents, contracting out the card production, managing the loading of identity data, card distribution, and revocation. The German government is responsible for the full e-ID 'lifecycle.' The US government relies on the private sector to supply online credentials to Americans. It owns no infrastructure for generic citizen electronic identity; some individual departments and civil agencies have their own authentication infrastructures. Its model is similar to procurement, defining product standards

for its needs. However, it is not paying for credentials. Consequently, the 'market' for citizen credentials is stillborn. At the time of this writing, the only credentials available to the general citizenry have little to no confidence in the identity behind them. This means that they cannot be used with e-government applications that exchange personal data as the credentials do not satisfy privacy requirements. German policy is more mature than US policy; 18.5 million e-IDs have been distributed as of February 2013. Only 28% of those have their online authentication capability turned on (Bundesverwaltungsamt, 2013). So, while Germany's credentialing efforts are far ahead of the US, the low number of activations hinders the policy intent to foster trusted, privacy-preserving online credentials.

This chapter finds that unlinkability is a policy choice derived of the principles of proportionality, minimum disclosure, and context separation. It is encoded into the formal and informal policies of Germany and the US, and into their credentialing technical architectures. It overlaps appreciably with requirements for pseudonymous online interaction. In this way, the research is also an appraisal of national pseudonymity policies. Identity management and e-ID policies are advancing privacy and data protection goals generally. Germany and the US are both incorporating technical forms of privacy enforcement based on cryptography. Unlinkability, a strategy to frustrate profiling and enhance user control, is specified in technical requirements, protocols and system architectures, as well as organisational operating constraints. In Germany, the unlinkability features of their e-ID card reinforce and reapply prior requirements in data protection and telecommunication law.

A comparison of the two countries' electronic citizen identity efforts and policies illustrates that German privacy and data protection is more 'coherent' (Righettini, 2011, p. 146; see also Busch, 2010) than the United States. Chapter 8 theoretically analyses the institutional dimension of both countries' data

protection and privacy regimes using the new institutionalist approach. The present chapter first compares the formal policies and laws of each country, policy implementation and the governing data protection model. Key policy actors are compared, as is the commercial aspects of policy implementation, which became a significant issue through inductive analysis of the case data. Finally, implementation challenges in the two countries are compared.

Policy requirements

There are several policy instruments that led to the US requirement for unlinkability. The Privacy Act of 1974 constrains federal agencies' collection and use of personal data. It requires data minimisation and proportionality by mandating that agencies shall "maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose …" (Privacy Act of 1974, Sec. e(1)). Many government stakeholders cited the non-binding Fair Information Practice Principles as a strong influence on citizen credential privacy requirements (G001, Interview; G003, Interview; G006, Interview; N005, Interview). With regard to data minimisation and proportionality, the FIPPs state:

> "Organizations should only collect [personally identifiable information] that is directly relevant and necessary to accomplish the specified purpose(s) and only retain [personally identifiable information] for as long as is necessary to fulfill the specified purpose(s)." (White House, 2011, p. 45)

One government lawyer (G006, Interview) noted the influence of the Office of Management and Budget's (2007) Memorandum 07-16, which requires the safeguarding of personally identifiable information:

> "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is

> linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."

All government agencies are required by the E-Government Act of 2002 to conduct 'privacy impact assessments':

> "… an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks." (Office of Management and Budget, 2003)

For credentials intended for e-government use, the Trust Framework Provider Adoption Process (ICAM, 2009d) defines the privacy requirements for participating identity providers (IDPs). It bans 'activity tracking,' stating:

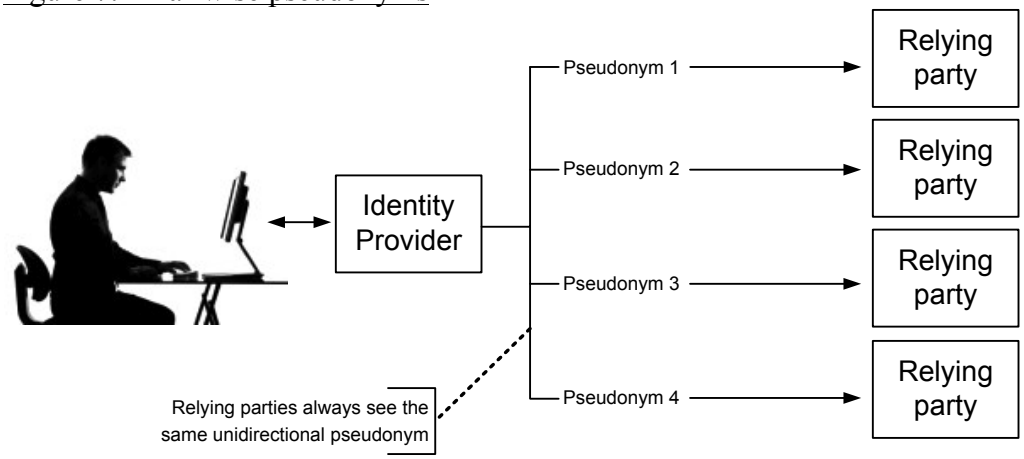
> "IDPs must not disclose information on end user activities with anyone and must not use the information for any purpose other than the federated identity service." (ICAM, 2009d, p. 12)

This requirement limits identity providers from using or disclosing information on which websites a user accesses with the IDP's credential.

The Federal Identity Credential and Access Management (FICAM) body defined three 'identity schemes' – protocol subsets of three identity federation standards: Secure Assertion Markup Language (SAML) 2.0, OpenID 2.0, and Identity Metasystem Interoperability (IMI) 1.0. The schemes are constrained configurations of the standards, encoding privacy and security requirements deemed necessary to interact with federal IT systems. SAML 2.0 and OpenID 2.0 are capable of sending a pseudonym to identify citizens instead of more identifiable information, such as a name or social security number. A different

pseudonym can be sent to each relying party, making the credentials unlinkable – these are called 'pairwise' pseudonyms.

Figure 7.1 Pairwise pseudonyms



FICAM's published specification for OpenID 2.0 requires the use of pseudonyms (ICAM, 2009b), and the SAML 2.0 specification strongly recommends them (ICAM, 2011a). There are no IMI 1.0 systems in production. All activity on the standard has ceased, and this research does not make further reference to it.

The Federal Cloud Credential Exchange, described further in the technical section below, currently exists as a request for proposals (RFP). One of its mandatory business requirements is:

> "The FCCX service shall support the privacy requirements of anonymity, unlinkability and unobservability." (United States Postal Service, 2013a, p. 5)

This requirement is expanded into mandatory prohibitions on identity providers having "visibility into customer transactions" carried out with other IDPs and relying parties, and prohibitions on relying parties having visibility into transactions in other relying parties (U.S. Postal Service, 2013b). The transactions in question are logins and activity on a federal website.

The German e-ID is authorised by the 2009 *Personalausweisgesetz*, the Act on Identity Cards and Electronic Identification. The Act does not mention pseudonyms. Instead, Technical Guideline TR-03127, published by the Federal Office for Information Security (2011), details the technical nature of the pseudonym function, and specifically cites an unlinkability intent:

> "The pseudonym is generated in such a manner that the pseudonym for one service provider cannot be used to derive a pseudonym generated for another service provider." (Federal Office for Information Security, 2011, p. 22)

The overarching policy governing privacy and data protection for online activities is the 2003 Federal Data Protection Act, amended in 2009; a required transposition of the 1995 European Union Data Protection Directive. The Act requires data minimisation, stating:

> "Personal data are to be collected, processed and used, and processing systems are to be designed in accordance with the aim of collecting, processing and using as little personal data as possible. In particular, personal data are to be aliased or rendered anonymous as far as possible and the effort involved is reasonable in relation to the desired level of protection." (Federal Data Protection Act, 2003, Sec. 3a)

As detailed in Chapter 6, the decisions of a 1983 Constitutional Court exert a strong influence on all German data protection. The court derived a right to informational self-determination, and mandated that the state cannot be considered a single entity in regards to the collection and processing of personal data (Hornung and Schnabel, 2009). These two decisions add context and a legal framework to all data protection activity (Hornung and Schnabel, 2009; Möller, Interview). By disallowing the state to act as a single data processor, the court mandated 'context separation' – data used in one civil context must be separated from other, disparate civil contexts. Unlinkability is a strategy to address this mandate by keeping contexts separate via different

pseudonyms. The court decision adds to the coherence of German data protection and privacy mechanisms underpinning the choices of its e-ID policies. The US lacks the legal weight of a court decision or law. Still, the 'spirit' of the German context separation is appearing within American policy. Citing the FIPPs' Use Limitation principle (White House, 2011, p. 45), a 2012 privacy framework released by the White House (2012, p. 15) calls for "Respect for Context": "Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data." The Privacy Coordination Committee (2013) of the steering group convened to help realise the National Strategy for Trusted Identities in Cyberspace outlines a variety of privacy harms including "Unanticipated Revelation": "Dissonance in the contextual use reveals or exposes person or facets of a person in unexpected ways." These non-judicial and non-legislative documents are public policy, albeit with stronger normative force than coercive, which are part of the formal influences that contributed to US unlinkability policies.

A legal precedent for pseudonymity requirements exists in the *Telemediengesetz* (Telemedia Act), legislation relating to e-commerce and "information society services" (Telemedia Act, 2007, Preamble). The Act requires the option for pseudonymous use of an online service:

> "The service provider must enable the use of telemedia and payment for them to occur anonymously or via a pseudonym where this is technically possible and reasonable." (Telemedia Act, 2007, Sec. 13(6))

The Act also cites a specific intent of unlinkability: "user profiles … cannot be brought together with details to identify the holder of the pseudonym" (Telemedia Act, 2007, Sec. 13(4.6)). Relatedly, a German e-signature law that pre-dated the European Union's e-signature directive allowed pseudonymous signing, although the same pseudonym was envisioned to serve for all interactions, rendering it linkable (Hornung, Interview; ULD, Interview).

For Germany, the online credential policy process-making was coherent given a prior national identification policy, an omnibus conception of personal data, strong pre-existing laws that emphasised pseudonymity, and a formal data protection policy layer in the form of state agencies and a federal commissioner. A German law specifically created both the e-ID and its online authentication capability. In the US, citizen credentials grew out of e-government and cybersecurity policy priorities rather than a specific authorising law. The US had to erect a new body of policy to realise its identity management goals, versus Germany who built their e-ID laws and policies upon pre-existing ones for national identification, telecommunications and e-signature. There was also a single German agency responsible for electronic identity, the Ministry of Interior. It was already responsible for the prior ID card, the passport and e-passport, and immigrant identification issues. It had introduced the e-passport immediately prior to the e-ID and had strong institutional ties to the German Parliament. The Federal Office for Information Security, who had technical oversight for identity documents, is the Ministry's sub-agency. Taken together, policy development of the e-ID, including its privacy requirements, was a coherent process. It took five years from the initial public announcement of the e-ID to the start of its distribution.

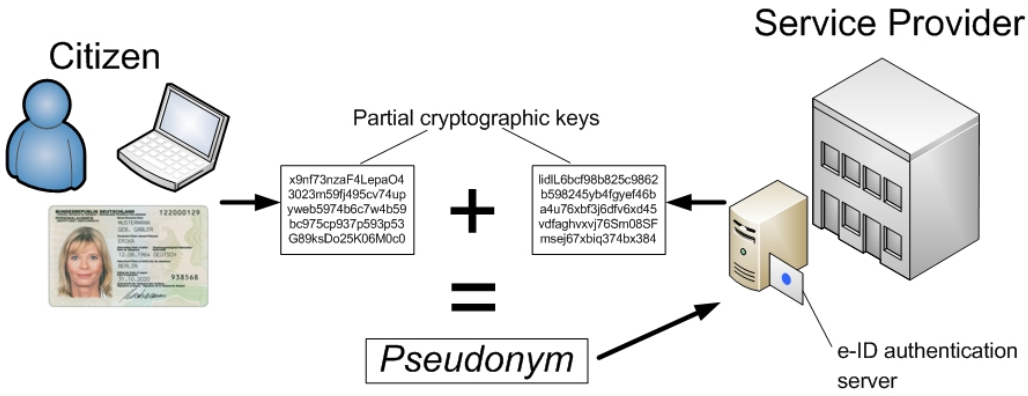
US credentialing efforts for citizens were less coherent than German efforts. Lacking an omnibus data protection or privacy framework, the US relied on administrative rules, sectoral legislation, and non-binding principles to form the privacy regime for electronic citizen credentials. All identity documents are governed by various parts of the Executive branch. Travel documents such as passports fall under the ambit of the State Department. The policies and organisational resources deployed for travel documents and federal employee identification had a very limited impact on general citizen credentialing; it was effectively started from scratch. The choice to rely exclusively on external

providers yielded a set of stakeholders with various and independent interests. Unlike the German Ministry of Interior, who had direct command over large swathes of e-ID policy and a strong influence on the other parts, FICAM and the other actors of US IDM policy development had limited influence on the implementation piece of the policy. Implementation from the identity provider side was in the hands of private actors. By not using the power of the federal 'purse,' those private actors had little incentive to meet government needs.

Technical implementation

Unlinkability in Germany is accomplished by the use of pseudonyms created from the union of two cryptographic keys: one held on an e-ID card and one contained within a certificate bound to an individual service provider. In combination, the two keys produce a unique pseudonym – it is 'card- and service provider-specific.' In the case of two different service providers, each with its own certificate, a unique pseudonym is produced for each provider.

Figure 7.2 The e-ID pseudonym generation process



When logging into two different websites with two different pseudonyms generated in this fashion, it cannot be determined that the same citizen is logging in. This is only true, though, in the absence of other linkable data, such as an email address.

The German government is unable to know which service providers citizens visit due to a lack of centralised servers in the e-ID architecture that could log online activity. This can be called 'unobservability'; the government is the assumed observer in this case (Pfitzmann and Hansen, 2010, p. 17). In unlinkability terms, the government is the identity provider – it issues the identity credential after vetting the claimed citizen identity at the time of enrolment. Whenever the credential is used at a relying party, such as an e-government resource, the identity provider is not aware of the usage. This arrangement distinguishes 'online' identity providers, where credential usage 'speaks' in real-time to the IDP's systems, and 'offline' providers, where credential usage is effectively severed from the originating IDP. The German system is an offline identity provider – the e-ID is a standalone credential, and its activities are not logged by its originating source. It was an intentional policy choice to avoid using centralising servers in the German e-ID architecture (Möller, Interview). During policy development, administrators reviewed the Austrian e-ID system and rejected it because of the linkability posed by centralised servers (Fromm, Interview).

The US technical implementation should be viewed in two stages: pre-FCCX and post-FCCX. The Federal Cloud Credential Exchange is in its earliest design stage at the time of this writing, existing as a set of requirements in an RFP, but its eventual deployment could greatly affect the use of unlinkable credentials by US citizens. The proposed FCCX is described as a 1-year pilot project (U.S. Postal Service, 2013a). The contract to build and maintain it was awarded to SecureKey Technologies, Inc., a Canadian identity management and security company, in August 2013 (SecureKey, 2013).

Pre-FCCX

In the original policy design of citizen-facing online credentials, unlinkability was technically accomplished by the requirement for each identity provider to use a 'pairwise' pseudonym with each different relying party. However, of the two identity protocols in use, SAML 2.0 and OpenID 2.0, only the OpenID 2.0 identity scheme *requires* pairwise pseudonym usage – the SAML 2.0 scheme leaves this as a recommendation. The ICAM OpenID 2.0 Profile (ICAM, 2009b, p. 18) states:

> "The pseudonym is used to identify the end user to the RP in a way that protects the end user's privacy by preventing propagation of the end user's common identifier throughout the Federal Government…. The IdP MUST construct a pseudonym in a way that ensures that it cannot be reverse engineered to help identify an end user across multiple realms."

This language is the most specific technical requirement for unlinkability in US public policy, except for the requirements for the as-yet unbuilt FCCX, detailed below. It mirrors the language in the *Telemediengesetz* in the preceding section regarding the option for pseudonymous internet use. In contrast to OpenID, the ICAM SAML 2.0 Profile (ICAM, 2011a, p. 20) states:

> "The use of pseudonyms (persistent identifiers) is strongly RECOMMENDED [*sic*]"

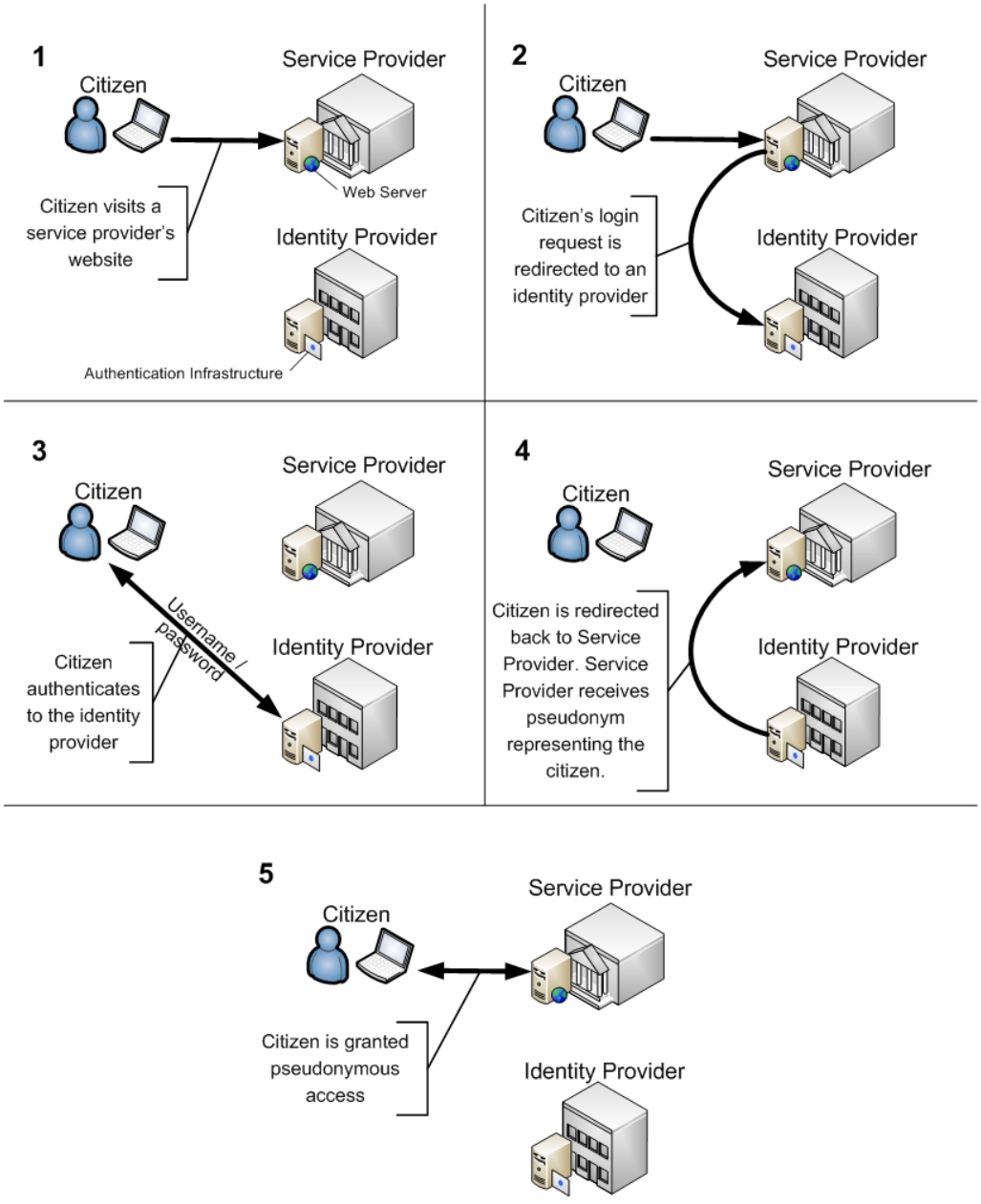
A senior government identity management administrator has acknowledged that the disparity between the two Profiles is a flaw:

> "That is not strong enough in my point of view, and I think we are actually going to be tightening up that language…." (G009, Interview)

The disparity is particularly problematic because the OpenID 2.0 Profile is only approved for Level of Assurance (LoA) 1 where there is little to no confidence in an asserted identity, but SAML 2.0 Profile is approved for LoA 1, 2 and 3; pseudonymous usage is acceptable up to LoA 2. For the

pseudonymity to have any real value to obscure a real identity, it must be used at LoA 2, which requires some confidence in an asserted identity.

Figure 7.3 The redirect method: User begins at service provider



Source: adapted from ICAM, 2011a, p. 10

The overall design for logging into relying parties using SAML 2.0 or OpenID 2.0 in the current, pre-FCCX period is called the 'redirect method' – requests to log in to a service provider are redirected to an identity provider. There are two use cases: a user begins her journey at a relying party, or the user begins at an identity provider. Figure 7.3 above illustrates the first case.

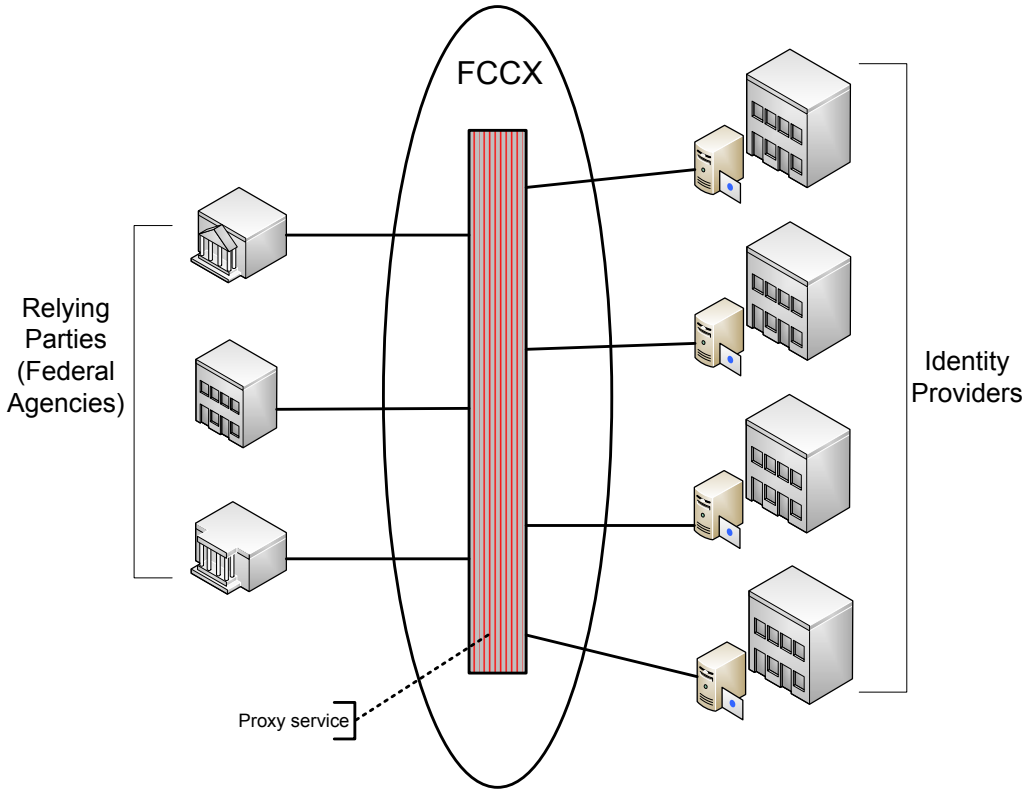
In this model, a citizen visits a service provider's website, e.g., an e-government resource. In order to log in, the citizen selects an identity provider with whom she has previously enrolled. The service provider redirects the login request to this identity provider. The citizen authenticates herself to the IDP. The IDP then sends confirmation of a successful login to the service provider, who grants access to the citizen. For transactions up to Level of Assurance 2, the IDP may send a pseudonymous identifier that represents the citizen instead of a linkable identifier, like a name or email address (Office of Management and Budget, 2003, p. 14). When this ceremony is performed at two different service providers, they each get a different pseudonym. The online interactions are, in the absence of other linkable data, unlinkable. In the second use case, where a citizen begins her interactions at the identity provider, the process is similar except that the selection of the IDP and the relying party are reversed. It is vital to note that in the redirect model the identity provider is aware of all of its credential uses. It knows each relying party the citizen visits, and maintains a mapping of all pseudonyms used at those relying parties. This is 'RP/RP blindness' – the relying parties cannot, in the absence of other linkable data, determine the identity of a pseudonymous user by colluding. However, a citizen's identity can be discovered by an RP colluding with an IDP.

Post-FCCX

Once the Federal Cloud Credential Exchange has been built, it will increase the federal government's ability to render citizen credentials unlinkable. The

FCCX is an intermediary layer between identity providers and relying parties. Its chief goal is to centralise and harmonise identity management efforts for federal agencies (G010, Interview). An additional benefit will be the ability to blind both sides of identity transactions, IDPs and RPs. Figure 7.4 below shows a simplified diagram of the FCCX.

Figure 7.4 Proposed Federal Cloud Credential Exchange



Computer systems inside the FCCX will receive credentials from identity providers and remove information identifying the credential's source (G009, Interview; John, 2012). This way, relying parties will only know that they have received a valid credential, but not know its origin. When the credential contains pseudonymous identifiers, two different relying parties will not be able to determine the identity of citizen – RP/RP blindness. However, the FCCX also prevents an identity provider from knowing the final destination

and use of its credential. All it knows is that it received a request for a credential from the FCCX. While the IDP maintains a mapping of citizens to pseudonyms, it does not know whom the recipient of those pseudonyms is – this would be IDP/RP blindness.

For citizen credentials envisioned by the National Strategy for Trusted Identities in Cyberspace – i.e., not for e-government use – policy development is still too formative to know what types of technical enforcement are feasible. The NSTIC is very clear about its unlinkability goals (See Chapter 5), but it remains to be seen how they will be realised.

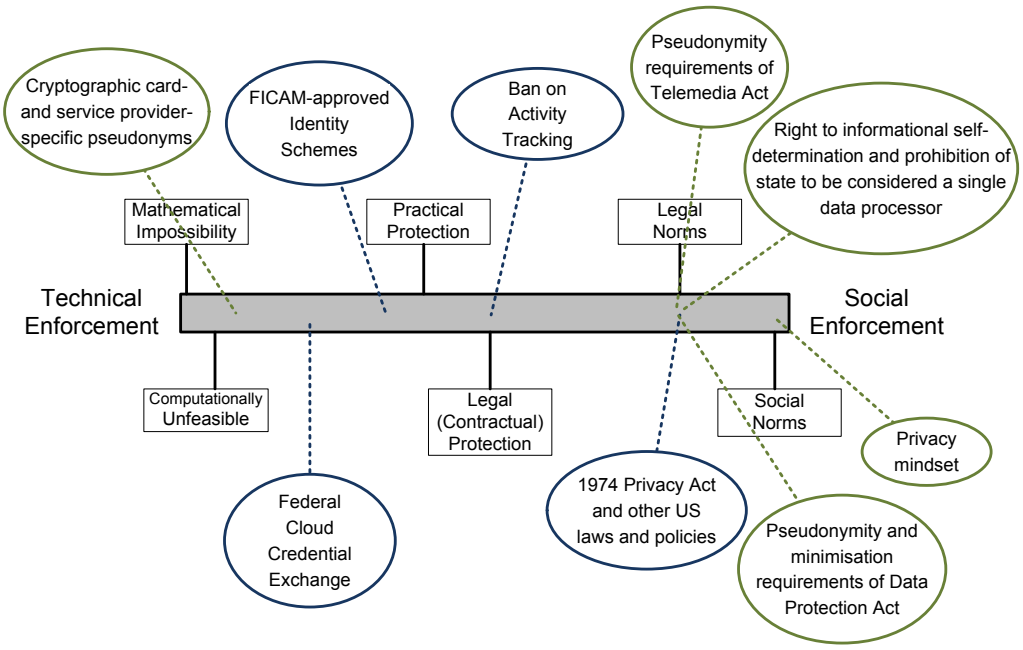
Data protection models

The German model of data protection for citizen-focused digital identities largely relies on technical enforcement. Protection of personal data stored on the e-ID is accomplished through cryptographic security measures. Cards divulge the data stored on them only in the presence of appropriate authorisation certificates. The biometric data on the card can only be accessed via readers in a face-to-face interaction; it is not possible to access or send the data in other ways (Fromm, Interview; DE-G005, Interview). For non-law enforcement access to the rest of the data on the card, a piece of software is required: the AusweisApp. This application, supplied by the government, sits between the citizen and the service provider wishing to read the card data. The card will only release the data via the application if the service provider has a valid authorisation certificate; see Chapter 6 for a complete explanation. Service providers obtain the legal authorisation to procure a technical certificate by applying to the Federal Office of Administration. This agency reviews the application to ensure that the service provider will request only the minimum amount of data needed for its service. In this way, non-technical policy mechanisms support technical ones. Unlinkability is achieved through

reliance on the service provider's authorisation certificate and a cryptographic key stored on the e-ID specifically to create pseudonyms.

The US model of data protection began with a mix of technical and social means of enforcement, but is now in the early stages of creating a stronger technical regime. Initially, data protection was driven by requirements and audits to ensure compliance. FICAM, the governing body for citizen credentials, required participating identity providers to have privacy policies comparable to the federal government's. Independent assessors, working under the banner of one of the Trust Framework Providers, certify that identity providers conform to the requirements. Additionally, technical interoperability must also be achieved. Identity federation relies on the use of standards, which can be configured in a number of ways. The federal government requires a constrained set of three standards to be used with government relying parties. The standards encode privacy goals to various degrees. One standard, OpenID 2.0, requires the use of pairwise pseudonyms in certain types of transactions, and another, SAML 2.0, recommends their usage. This is the greatest degree of technical enforcement of unlinkability in the extant citizen credentialing system for e-government access. Identity providers learn about their users' online activities through normal use of the system. FICAM rules require IDPs to keep this information confidential and not use it for other purposes, such as marketing. Ergo, for the data protection model to work, audits must be comprehensive and IDPs must not lie about their operations. Compared with Germany, where no IDP is aware of credential uses, this is a weaker form of privacy protection. Drummond Reed's spectrum of unlinkability, discussed in Chapter 5, illustrates the how different data protection influences based on different methods of enforcement yield the unlinkability policies of Germany and the US. The figure below combines US and German policy instruments and influences that contribute to their respective policies of unlinkability.

Figure 7.5 Reed's Spectrum: US and German policy instruments and influences



US identity management policy administrators realised that they would need to assist agencies to meet their mandate to accept externally-issued credentials:

> "Agencies have been challenged … due to technical, policy and cost barriers that have made it challenging to accept third-party credential providers accredited by the Federal Identity, Credential, and Access Management (FICAM) initiative." (U.S. Postal Service, 2013a, p. 4)

In January 2013, a request for proposals was released to gather bids to build the Federal Cloud Credential Exchange. The FCCX will contain most of the infrastructure needed to accept various credential types from a plurality of identity providers. The requested system design requires unlinkability: identity providers are to be blinded from the uses of their credentials, and relying parties are to be blinded from one another. This technical means of enforcement, when built, enhances US identity management privacy goals further than previous policies. The FCCX RFP states:

> "Specifically, the FCCX service must limit loss of anonymity, unlinkability and unobservabilty." (United States Postal Service, 2013a, p. 5)

This requirement is ambitious and far-reaching – the FCCX design proposal also requires a capability to support 135 million users (U.S. Postal Service, 2013b).

Until the FCCX is built, unlinkability goals in the US will be satisfied by social enforcement upon private actors who will then technically and socially enforce the goals. FICAM requires (social) participating identity providers to configure their systems to produce pairwise pseudonyms (technical), and not share the information they learn of a citizens online activity (social). In contrast, the German system relies more on technical enforcement. Cryptography on the card and within the e-ID system creates pairwise pseudonyms, and the overall architecture renders the system unobservable to the government. However, there is no overarching requirement in Germany for organisations to use pseudonymous logins. Instead, such use occurs when an organisation deems that a particular online service could function pseudonymously. When the FCCX is built, technical enforcement methods will supersede social ones, and the US commitment to unlinkability will rival or surpass Germany's.

Actors

Regarding electronic identities for citizens, one agency in Germany is responsible for making policy, but in the US policy-making has been more diffuse. In Germany, identity and travel documents fall under the ambit of the Ministry of Interior. It has been the primary actor in evolving Germany's original paper ID into the current e-ID. Its sub-agency, the Federal Office for Information Security, was responsible for the technical architecture of the system, having designed the e-passport system immediately prior. A different sub-agency, the Federal Office of Administration, was responsible for

developing and managing the data protection model for accessing citizen data on the cards. Federal and state data protection authorities contributed to the development of the privacy and data protection principles embedded within the e-ID through direct consultation with the Ministry. Local municipality offices played a role by being the first point of citizen contact and the distribution point for finished e-ID cards. Also, the increased administrative burden of registering citizens for the e-ID caused the municipalities to raise cost objections to the Ministry, who subsequently tripled the cost of the e-ID from the cost of the previous ID card (Fromm, Interview; Kubicek, Interview). Still, the Ministry of Interior unquestioningly drove the e-ID process, wrote the majority of its authorising law, and managed the rollout of the cards. It took five years from the first public discussion of policy to card deployment.

A central figure in the policy development of the e-ID was Jan Möller, a lawyer within the Ministry of Interior. He was hired specifically to work on e-ID issues. Prior to joining the Ministry, Mr. Möller worked for the ULD, the data protection authority of the state of Schleswig-Holstein. His experience at the ULD helped shape his views regarding privacy and identity (Kubicek, Interview; Möller, Interview), ultimately influencing the data protection principles embedded in the *personalausweis*. At the Ministry, Mr. Möller was a key actor in the design of the e-ID law and in the policy interaction between the German Parliament and the technical agencies responsible for building the e-ID architecture. Under Mr. Möller's direction, the e-ID design included a selective disclosure feature for age and locality, and the pseudonymity function to enable unlinkable logins.

German academics and researchers also played a role in the development of e-ID policy. Herbert Kubicek, a University of Bremen scholar, researched the e-ID during its formative policy development and has provided research to the Ministry of Interior (Kubicek, Interview). Gerrit Hornung, a law scholar of

electronic identity issues at the Universities of Kassel and Passau, and Prof. Dr. Alexander Roßnagel of the University of Kassel participated in feasibility studies and other research on behalf of the government (Hornung, Interview). The Technical University of Darmstadt was involved in pilot studies of the card technology (DE-G005, Interview), and the Fraunhofer research institution served in an advisory capacity (Fromm, Interview).

In the US, the Executive branch of government has driven identity management efforts. Besides electronic citizen identities, parts of the Executive branch have engaged in multiple identity initiatives. These include a passport card (in lieu of the traditional booklet), the Transportation Worker Identification Credential, and the personal identity verification (PIV) card for federal employees and contractors. Travel-related documents fall under the ambit of the State Department. Physical and online identity management initiatives fall under the remit of the Federal Chief Information Officers (CIO) Council, an inter-agency council comprised of the chief information officers of Executive branch agencies and the intelligence and military communities. The Identity, Credential, and Access Management (ICAM) subcommittee of the CIO Council has direct responsibility for identity management issues within government-to-government, government-to-business, and government-to-citizen interactions (ICAM, 2009c). FICAM (the 'F' is added for 'Federal') is staffed in part by members of the General Services Administration, who assists in the implementation of government-wide policy for the Executive branch, as well as by representatives of the Department of Defense (G001, Interview). Privacy policy for government-to-citizen credentialing was overseen by members of a privacy subcommittee of the CIO Council who formed an identity management subcommittee for the task (G006, Interview; G010, Interview). On this subcommittee was Naomi Lefkovitz, a privacy lawyer who previously was Senior Attorney for the Division of Privacy and Identity Protection at the Federal Trade Commission and the Director for Privacy and

Civil Liberties of the Cybersecurity Directorate at the White House. Ms. Lefkovitz was also one of the core authors of the privacy language in the NSTIC and is a key privacy figure in the development of the FCCX (G010, Interview).

While Ms. Lefkovitz and Mr. Möller certainly did not act alone – both were part of multi-agency teams and worked in concert with other lawyers, administrators and technologists – they are central figures in the policy evolution of unlinkability. They and their colleagues are part of a small number of individuals directly responsible for the evolution of privacy within identity management, and, it is argued, privacy and data protection as a whole within their respective countries. Mr. Möller was given great latitude in his development of the privacy features of the German e-ID:

> "[The Ministry] hired Möller to take care of the privacy issues. And my impression is that they didn't really care what he proposed because they believed in him.…" (Kubicek, Interview)

Ms. Lefkovitz and her colleagues Debbie Diener and Toby Levin distilled the Fair Information Practice Principles into the FICAM privacy requirements for citizen credentials (G006, Interview). As one of the authors of the NSTIC privacy language, Ms. Lefkovitz further derived the FIPPs into very specific unlinkability goals. For example, the NSTIC explains the 'driver's license model,' highlighting how privacy can be maintained by severing information links between organisations:

> "The offline world has structural barriers that preserve individual privacy by limiting information collection, use, and disclosure to a specific context. For example, consider a driver's license: an individual can use a driver's license to open a bank account, board an airplane, or view an age-restricted movie at the cinema, but the Department of Motor Vehicles does not know every place that accepts driver's licenses as identification. It is also difficult for the bank, the airport, and the movie theater to collaborate and link the transactions together." (White House, 2011, p. 11)

The privacy features of the German e-ID and the American FCCX's requirement for unlinkability are the most advanced citizen-facing privacy and data protection policies in their respective countries. In this way, identity management policy is advancing data protection and privacy generally. The contemporary needs for strong authentication and the introduction of new technologies to meet those needs caused reinterpretations and extensions of earlier data protection and privacy principles, specifically proportionality and minimisation. Ms. Lefkovitz and Mr. Möller are parallel, key agents of data protection and privacy evolution. They and their colleagues are responsible for a greater use of privacy-enhancing technologies – in this case, cryptographically-based unlinkability – in public policy.

The Trust Framework Providers (TFPs) are actors in their own right, though, as discussed in the institutional analysis in Chapter 8, they serve as intermediaries. As FICAM was developing the Trust Framework model, policy was iterative, and the Trust Framework Providers themselves contributed to the shape of the policy (Thibeau, Interview; N004, Interview). The US government committed to the Trust Framework model, and therefore needs the TFPs to implement IDM policy.

The Trust Framework Providers are necessary to bridge US government requirements to external identity providers. There is no equivalent in Germany as the government itself is the only identity provider. There is no evidence that academics were consulted during US policy development, as opposed to Germany, who additionally could rely on the input of federal and state data protection authorities, a policy layer absent in the US. These two additional voices in German policy development evince a greater degree of data protection coherence than the US.

Technical support for cybersecurity and identity management policy came from the National Institute of Standards and Technology. Much like the German Federal Office for Information Security, NIST was responsible for development and approval of cryptographic standards and technology for use in federal IT systems. Standards organisations such as the OpenID Foundation and OASIS, responsible for the SAML protocol, were also actors within IDM policy development. As discussed in Chapter 5, the OIDF membership declined to work directly with the US government on its identity management needs and instead spawned a separate organisation, the Open Identity Exchange, to address those needs. OASIS was obliquely related in that its members' values and norms infuse the SAML specification, as discussed in the institutionalist analysis of Chapter 8.

Commercial influences

German and US identity management efforts are both affected by commercial considerations, which in turn affect the implementation and use of unlinkable credentials. In the US, the market and commercial organisations are critical factors since the government is not willing or able to deploy its own citizen credentials. By choosing to rely on private organisations to supply credentials, government policies are intrinsically bound to the logic of the market: returning shareholder value, profits, building for multiple markets, reduction of costs. So far, the lack of a business model that could yield sufficient revenues for commercial IDPs has held back the creation of high assurance credentials for use with e-government. In Germany, credential issuance business models are not a problem because the government is itself the issuer. However, private organisations are not interested in becoming certified to access the data on the German e-ID because the cost is not justified. Companies that operate internationally do not have incentive to pay for the certification because the value of verified card data versus volunteered personal information is not perceived to be high enough.

Regarding unlinkability, German citizens can gain its benefit only when the owner of a website becomes certified to access the e-ID data. When credentials are to be used with e-government sites, commercial logic is diminished in favour of mandates to engage more citizens, reduce interaction costs and improve service delivery. A return on the investment in the certification process is subsumed by the logic of e-government. However, policy intentions to provide citizens with a trustworthy online credential for use with commercial entities are frustrated by the lack of incentive for private actors to participate in the e-ID system.

For the US, citizens will not get online credentials at all for meaningful e-government use until the business case is satisfied. It may come to pass that different government agencies pay for credentials for their client populations, giving commercial identity providers incentive to deploy systems, but this has not yet occurred. For the InCommon Federation, comprised of higher education and research organisations, the profit motive is mitigated, though cost is still a factor. InCommon members, such as Virginia Polytechnic Institute and State University, are beginning to become identity providers certified to FICAM requirements. Their mandate is to serve their student and researcher populations (Morgan, Interview), and enable easier access to e-government resources, such as those built by the National Institutes of Health. Certification of higher education and research organisations is still burdensome, though, and there are differences of opinion as to the appropriateness of government privacy imperatives in the higher education and research space (Morgan, Interview). Further, it is still unclear how valuable federally approved credentials are to those organisations. Bob Morgan (Interview), a senior technologist at the InCommon Federation explained:

> "… is it a significant university use case to use your university ID to go to the IRS and do tax stuff? If that's gonna increase my risks – it sure

> sounds like it is – then I'm not interested in even doing that, right? It's certainly not in my mission."

One other commercial issue of note is the influence of the companies that build and manage identity card systems, what David Lyon calls "the card cartel" (2011, p. 16).

> "The forces driving national ID card systems are like a combination of firms that get together to keep prices artificially high and to keep out competition." (Lyon, 2011, p. 68)

Lyon ties the growth of national ID card projects after 11 September, 2001, to the longer history of government procurement of security and surveillance infrastructure from private sources. The 'hand-in-glove' relationship between states and commercial interests helps to explain the similarity of ID initiatives in disparate countries:

> "… the card cartel theory helps to explain … why ID card systems of strikingly similar kinds are introduced despite deep political controversies over the acceptable rationale for them." (Lyon, 2011, p. 80)

The development of the German e-ID cannot therefore be fully understood without accounting for influence of the 'oligopoly' of commercial interests intertwining with technological and government pressures. Lyon (2011, pp. 82-83) notes:

> "Different pressures, at once governmental, commercial and technological, converge to make the development of ID card systems seem like a 'solution' to several perceived problems at once."

It is unclear if Lyon's cartels extend to US credentialing efforts, but his theory adds context to the German case. It could potentially help explain the swiftness of the e-ID deployment and the explicit policy desire to change the size of the e-ID to the more common ID-2 format. That isomorphic physical characteristic

could arguably be explained by the commercial logic to build similar products for the widest possible range of government customers.

ID cards and digital identities are products, and are therefore imbricated in commercial prerogatives. Since US credentials originate from private sources, the choice to include unlinkability is also ultimately commercial. That is, for a private organisation to issue credentials the government can accept, it must choose to include unlinkability in its product architecture. In the German case, the inclusion of unlinkability is distanced from commercial considerations because the credentials originate with the state who needs no commercial mandate for privacy.

Implementation Challenges

The key challenges facing both countries relate to credentialing generally, not unlinkability specifically. In Germany, the main challenge is the high number of citizens not activating their e-IDs' online authentication function. As of 28 February 2013, 18.5 million e-IDs have been distributed, and only 28% have their online authentication function turned on (Bundesverwaltungsamt, 2013). This low usage thwarts the policy intention to facilitate trustworthy transactions on the internet in a privacy-preserving manner. The goal of enabling pseudonymous logins cannot be realised if citizens do not use the e-ID online. Some German administrators believe that the key reason the online authentication function is not being used is marketing – citizens do not know what they can do with it, and municipal agents who are the first and last point of contact for the e-ID do not have a reason or enough knowledge to recommend it be activated (DE-G002). Jens Fromm of the Fraunhofer Institute observed that government may have been overly ambitious in its expectations of the breadth of e-ID use:

> "The hope was in the beginning … that this card would be widely used for all kinds of services, not only … in initial identification, but as it

> was a marketing slogan in the beginning, 'one for all.' And there was a key, many keys, and there was the German ID card and all keys around this card. This was in my opinion a wrong view, a wrong expectation. But this was in some people's mind, their expectations in the beginning when we were thinking and starting this whole process…." (Fromm, Interview)

Relatedly, he also questioned the e-ID's value to a citizen (Fromm, Interview). The relatively low number of websites that accept the e-ID as authentication highlights the issue of value: 65 commercial sites and 40 e-government sites (Bundesverwaltungsamt, 2013). The challenge lies in the business case for commercial entities. The authorisation process to obtain a certificate to get data from the e-ID involves cost and staff focus. So far, the value of gaining access to verified, official data about German citizens and residents versus relying on traditional sources of that data remains unclear.

For the US, the challenge is somewhat greater in that citizen credentials for high assurance transactions have barely begun to appear. The key implementation challenge is the lack of a business case for identity providers to invest in high assurance credentials. As detailed above, the cost and complexity do not yet have an attractive return on investment. In the higher education domain, the case has not yet been made for universities to pay to become certified for their credentials to be used in Level of Assurance 2 transactions. The cost and constraints are not yet justified for many universities to participate (Morgan, Interview).

Both US and German identity management efforts face a challenge of usability, documented in Chapters 5 and 6. Pinch (2008, p. 474) observes:

> "A technology may succeed or fail depending on how well users are able to operate it."

There is widespread agreement that privacy-preserving credentials are conceptually complicated and difficult to present in easy-to-use ways (G007,

Interview; Morgan, Interview; N006, Interview; P001, Interview). This difficulty and complexity increases the likelihood that users will not understand their options, or even care to exercise them. IDM expert Paul Trevithick (Interview) observed:

> "Privacy and unlinkability and things like that … aren't baked into the fabric so it requires you to take *extra* steps to do things, install things in your software, and it's a very small percentage of the end-user market who will take a proactive step for an uncertain long-term benefit."

Also, there is a danger that user needs will be assumed rather than investigated in the design of identity management systems:

> "The needs and concerns of citizens or customers are often assumed by those commissioning and designing the identity solution, rather than researched." (Rahaman and Sasse, 2010, p. 607)

A fundamental challenge to a central goal of unlinkability – frustrating profiling – is the common use of linkable identifiers in online transactions. In e-commerce, citizens must supply a form of payment which invariably contains linkable identifiers like name, phone number and email address. In e-government, many meaningful interactions, such as reviewing available benefits or submitting medical claims, require strong authentication to defeat fraud and comply with privacy laws. In basic web interactions, sites often want to communicate with users when they are not visiting the site, so email addresses are requested. Email addresses are, in the words of Bob Morgan (Interview), the "currency of the realm." The internet is suffused with linkable activity. With regard to online payment, the use of anonymous cash is impossible, and anonymous forms of payment such as BitCoin are in their infancy with no guarantee of survival. Basic commerce requires in the least a method to contact customers in case of problems with an order; this means a linkable identifier. As such, it is not clear that unlinkability will gain traction in the identity market. If the 'standard operating procedure' of the internet is

linkability, the goal of unlinkable interaction may face an insurmountable uphill battle. One identity management expert opined:

> "I guess the questions are, 'Is there a real use case for unlinkability and … who's trying to be protecting who from [whom]?' Until we have clear answers for that, it's really hard to design any kind of technical solution…. if you ask the privacy people, they think that it is super important but don't necessarily understand all of the issues; they're … putting a big padlock on the door but the door is made out of tissue paper." (N003, Interview)

This issue may be the greatest challenge to using unlinkability as a privacy strategy. The internet is a highly linkable 'place.' Linkages infuse data with value. There are many times when linking is desirable, for efficiency or fraud detection, for example. Paul Trevithick's quote above is also salient: extra steps reduce the likelihood of use. Privacy-protecting technologies may need to be more invisible to be effective. These are the early days of PETs as public policy, and there will no doubt be many stumbles and iterations before realistic, feasible privacy policies can be enacted in such a way as to cooperate with market forces and the way people naturally use the internet.

Defining Identity Management Policy

Comparison of the two countries helps to build a definition of 'identity management policy.' Given the heterogeneous and sometimes contested boundaries of information policy (See Chapter 2), defining this sub-field is a useful exercise. Nominally, it includes issues related to government use of identity management systems. This subsumes, then, digital identity credentials and their lifecycle: citizen (or resident) enrolment, acquisition of identity and attribute data, credential use, problem resolution, and deactivation. Identity management policy includes specific technical architectures and procurement practices. It also includes privacy policies and system configurations. All of these topics are visible in the two cases, but identity management policy can be drawn more broadly. The US case demonstrates how digital identity is tied to

risk management via the Levels of Assurance framework. This framework is a crucial plank within IDM policy – the viability of federal agencies accepting external credentials is premised on it. While this kind of framework is not necessary internally within Germany, Germany is member of the European Union which is constructing a legal framework for the interoperability of electronic identities across its members' borders (EC, 2012). The EU framework addresses the same problem that the US Levels of Assurance does: the challenges in trusting authentications based on identity systems originating outside a host government. An EU project called Secure Identities Across Borders Linked (STORK) has developed a methodology similar to the Levels of Assurance called Quality Authentication Assurance (Hulsebosch, Lenzini and Eertink, 2009). German companies and agencies have participated in STORK, and Germany will ultimately be subject to any EU Directive that includes e-ID interoperability requirements. IDM policy therefore must include national, international and supranational issues related to interoperability as well as risk management frameworks.

Identity management policy concerns digital identity credentials generally – this means both online-only credentials, such as those envisioned by US policy, and physical credentials as with the German e-ID. By extension, IDM policy includes government use of credentials for non-internet-based transactions, such as electronic ID cards for physical entry into restricted areas and credentials for government employee access to electronic resources. This would subsume the US government's Personal Identity Verification card system for federal employees and contractors, and the Transportation Workers Identification Credential used for secure access to ports and maritime vessels.

IDM policy also includes e-signature policies. While e-signature is used as an electronic version of a handwritten signature to signal legal intent, it also has technical capabilities to authenticate the signer. The EU's 1999 Directive on

electronic signatures recognised this and created law to support the acceptance of e-signatures as proof of identity (EC, 1999). In the US, the Government Paperwork Elimination Act (1998, Sec. 1710(a)(1)) defines an electronic signature as "a method of signing an electronic message that … identifies and authenticates a particular person as the source of [an] electronic message." In the early days of Germany's identity management efforts, e-signatures were relied on for authentication until it was realised that German certificates did not contain enough information to fully individuate someone with a common name (Kubicek, Interview). The current draft EU regulation to replace the 1999 e-signature Directive is an attempt to build a "comprehensive EU cross-border and cross-sector framework for secure, trustworthy and easy- to-use electronic transactions that encompasses electronic identification, authentication and signatures" (EC, 2012). While there is an argument to be made that signalling legal intent is not identity management *per se*, e-signature technology and use militates its inclusion in identity management policy topics.

Identity management policy also includes the facilitation of 'trustworthy' credentials for general (i.e., non-governmental) use. Both US and German initiatives include this as a policy goal. The German e-ID's online authentication was designed expressly with government and business considerations in mind, and the US National Strategy for Trusted Identities in Cyberspace is aimed non-governmental usage.

A synthesis of the above discussion yields a definition of identity management policy: *Identity management policy is the set of laws and policies enacted by governments and supranational bodies concerning the facilitation, procurement, use, liability, legal nature, interoperability, technologies, risk methodologies, lifecycle and privacy of digital identities for its citizens and employees. This includes physical and logical authentication, e-signature, and*

electronic identification technologies for access to physical and electronic resources.

Conclusion

This chapter compared the similarities and differences of US and German policies regarding the option for unlinkable credentials. The formal policies, influences and technical implementations were compared, as well as each country's data protection model, the main policy actors, the commercial dimension, and key challenges each country faced in its implementation. It found that German data protection policy coherence led the country to reapply and extend core principles in the construction of e-ID policy, yielding a capability for unlinkable logins in the e-ID. Despite a less coherent data protection and privacy regime, US policy-makers and administrators interpreted the same data protection principles and promulgated requirements for unlinkability in privately-originating citizen credentials. In a proposed, unbuilt identity management infrastructure, unlinkability is required and strengthened above current policies.

German identity management policy is more mature than the equivalent US policy. Chiefly, this is because the German government is supplying its citizens with credentials in the form of an e-ID. The US government is soliciting private actors to supply credentials. As yet, none exist for the general citizenry than can be used in e-government interactions that require confidence in an asserted identity. Private actors lack incentive to build and configure their systems to meet federal requirements because no viable business model has yet emerged for general citizen use. Germany lacks the need for a business case for credential issuance, and 18.5 million cards have been issued at the time of this writing. However, German policy intentions for the e-ID to be used in commercial as well as e-government interactions are thwarted by commercial organisations' lack of interest in becoming certified to interact with the e-ID.

Only 28% of issued cards have their online authentication feature turned on (Bundesverwaltungsamt, 2013).

In both Germany and the US, a single lawyer has had a wide influence on privacy considerations within citizen identity management. Private government consultants have had strong influence on US identity management policy. Both governments are technically enforcing their privacy goals, and both identity management programmes are challenged by the conceptual complexity of pseudonym use and the difficulty of building usable technologies for a general populace.

The online authentication features of the German e-ID were carried forward by the larger policy goals of updating the German national ID card. Throughout the 2000s, many European nations updated their IDs to e-IDs. There was a 'fair wind' for this kind of policy. Or, according to Lyon (2009), an oligopolistic 'card cartel' strongly influenced many nations towards such a policy. In any case, online authentication was nested in a set of other policy issues that had their own momentum. It could be argued that the e-ID was going to be issued irrespective of online authentication considerations. This point is important when coupled with the implementation of the system. The bureaucrats in charge of the e-ID did not have to wait for relying parties to exist. On the contrary, until the Ministry's sub-agency, the Federal Office of Administration, defined the authorisation regime to allow organisations to read data from the card, no relying party *could* exist.

Compare this to the US model: an 'ecosystem' must be created, with IDPs and RPs appearing at the same time. That is, federal agencies (relying parties) need to build authentication infrastructures to consume credentials from IDPs. If there are no IDPs offering useful credentials, why spend money and focus? On the other hand, IDPs are commercial companies and universities, external to

government. They need a justification to invest in system alterations to meet federal requirements. If there are few relying parties, and no sustainable business model has emerged, why alter the systems? In the German model, the government did not have to wait for relying parties. It could just go ahead and release the e-ID card; the online authentication function was secondary. In the US model, without RPs there will be no IDPs, and vice versa. As a result, the policy is stalled. The Federal Cloud Credential Exchange is an attempt to redress this. When built, it will do most of the 'heavy lifting' involved in building an authentication infrastructure for US agencies. Ostensibly, this would speed up the addition of RPs to the ecosystem, creating a more favourable market for IDPs. The key to all of this is how IDPs will make money. The ecosystem – which serves government goals but not necessarily market player goals – hinges on commercial IDPs being able to make a profit.

The US IDM policy environment is one of 'use case vs. business case,' and it illustrates a tension in uniting citizen identification issues with commercial prerogatives. There is certainly evidence that the US would have had tremendous political difficulty in issuing a government-based citizen identity scheme. Nonetheless, meaningful e-government services cannot appear on a national scale until credentials do. Reliable credentials faithfully bound to the correct person are expensive and, so far, do not appear to constitute a market unto themselves. Given that these credentials are organisationally derived and managed, they may also only be relevant to the needs of particular organisations: Google logins are only useful to Google's marketing strategy, university logins are only useful to universities' goals. The German e-ID represents government interests and follows a path laid down by prior policy. The US IDM case may represent a failure of the plan to cross-pollinate private organisational interests with government interests. The UK has erected a policy similar to the US, the Identity Assurance Programme, relying on externally-provided credentials for e-government access (Gov.uk, n.d.). The key

difference is that the UK government is paying those providers. The US may have no recourse but to follow suit.

The comparison of German and US identity management initiatives helps to identify the contours of national identity management policy. By uniting the technical and policy features of the initiatives, a definition of identity management policy could be offered. The output of a definition for this heretofore undefined policy area illustrates the value of the comparative method in identity management research.

CHAPTER 8: APPLYING NEW INSTITUTIONALISM TO UNLINKABILITY

A core contribution of this thesis is the application of new institutionalist approaches to data protection and identity management. Information policy suffers from fragmentation in both its policy-making institutions and its resultant policies (Rowlands, 1996; Browne, 1997a). Accordingly, information policy research "needs to examine the component interactions not only within, but between policy contexts" (Trauth, 1986, p. 43). Such research benefits from an interdisciplinary approach, including perspectives from business, law, sociology, information systems, political science and computer science. These perspectives fit comfortably in the broad church of institutionalist thought. This chapter answers the calls of scholars to attend to the theoretical – specifically, the institutional – concerns of information policy research, and to examine the role of values and norms in policy-making. It applies the propositions at the end of Chapter 2 to the empirical case data to help explain the emergence of unlinkability.

Identity management and e-ID policies overlap with privacy and data protection regimes. Complementary and competing prerogatives of the state and the market, the tacit pressures of culture, and the inexorable progress of technology exert their influences on policy-making in the two case studies. By separating these influences and analysing their variable effects, it becomes clear that citizen identity management is subject to multi-stakeholder governance, and is affected by informal factors as much as formal instruments. The choice to include unlinkability in citizen credentialing architectures reflects history, technology, culture and power. New institutionalism is particularly helpful in this respect. It draws out the values embedded within these influences and highlights the relationships among actors, partly explaining the appearance of one policy versus another. It recalls the policy

choices of the past and illustrates how they affect the decisions of the present. This 'path dependence' is evident in the case data: Germany's e-ID is constrained by court decisions of 30 years past; US identity management policy is affected by legislation 40 years old.

Equally important are the cultural values embedded in IDM technologies. Institutionalist approaches are valuable in understanding the interplay of the cultural and the material. The German e-ID and concomitant US IDM technologies cannot be fully understood without considering their institutional role. "[M]ateriality itself exercises a form of agency," Pinch (2008, p. 466) writes. As such, the cryptography of US and German IDM systems constrain and enable social action. Their data protection functions reflect the logic of the market, the pressures of data protection regimes, the process of policy-making, the power of policy actors, and the cultural expectation that personal data is sensitive and worthy of being safeguarded. In order to understand information policy's effect on society, Braman (2009, p. 5) argues that we ignore its normative dimension at our peril. Institutionalist analysis enriches identity management research by focusing on the norms, values and informal aspects of information policy-making, the relationships among actors and technology, the visible and the invisible. There is limited application of new institutionalism to identity management research; this thesis addresses that gap. The research was conducted to better understand the role of public policy in the growing digital identity layer of the internet, and the formal and informal forces that shape data protection instruments brought to bear in that space.

Germany and the US have different policy histories and environments. Without direct policy influence on one another, both have promulgated policies that require the availability of unlinkable online credentials for its citizens. Unlinkability is a form of data protection, in service of privacy goals, and the two countries have substantially different data protection and privacy regimes.

Germany has a national, omnibus data protection law that transposes the supranational EU Data Protection Directive, plus a similarly transposed law on telecommunications and internet services. Citizens must legally possess a national identity card or passport beginning at age 16. The United States, at the federal level, has a set of sectoral privacy laws and a non-binding set of Fair Information Practice Principles. There is a strong antipathy towards national identity schemes due to fears of an overly intrusive state, and it is politically difficult for the government to furnish its citizens with online credentials, even for use restricted only to e-government access. The US lacks a data protection policy layer, versus Germany who has both federal and state level data protection authorities. The US lacks the "institutional coherence" (Righettini, 2011, p. 146) of Germany with regard to data protection. Given these differences, the reasons that both countries adopted a policy of unlinkability for its citizen credentialing are not immediately obvious. The policy histories, inputs and outputs, and environmental pressures alone do not explain the parallel appearance of unlinkability. Approaching the two cases theoretically helps to better understand the influences that led to a similar policy choice in two separate polities. Institutionalism in particular enriches scholarship on data protection and issues pertaining to electronic identity by drawing out the informal influences of norms, values, culture and relationships.

New institutionalism argues that policies cannot be understood without an examination of their institutional dimensions. It attempts to illustrate the link between "problems, politics and policies" (Weir, 1992, p. 191). As such, it assists the twin goals of information policy research: better understanding of existing information policies, and the utility to improve policy-making. Governments historically struggle with information policy because of its complexity and rapid evolution (Browne, 1997a; Reidenberg, 1997). IDM and e-ID in particular are complicated subjects, and their privacy dimensions are heterogeneous and broad in scope.

Electronic identity management of citizens is affected by data protection and privacy policies. In turn, it also affects them both. This dualism and IDM's complex, diverse set of technologies, goals, policies and actors are well suited for a theoretically enriched analysis. In the present research, multiple institutions and their subject organisations envelop the actors, choices and influences that yielded unlinkability policies. In IDM, the fields of e-government and national identification interplay with market actors, cybersecurity imperatives, legislatures, various communities of practice and national culture. A new institutionalist approach can begin to examine some of the forces and influences at work that a comparative analysis of the formal policies and implementation challenges alone would not reveal. Application and analysis of the propositions in the next section illustrate that the policy development of unlinkability is inseparable from its institutional context.

There is limited academic research on data protection as an institution. Literature discusses data protection authorities (Burkert, 1981; Righettini, 2011) and policy formation (Bennett, 1992) rather than considering the whole of data protection an institution. The discussion of the institutional nature of data protection in Chapter 2 and the institutional analysis of this chapter are part of the main contributions of this thesis. The findings help answer the central research question: How is unlinkability emerging as public policy? The analysis also answers the questions, what does identity management policy do to the institution of data protection, and what does it take from it?

This chapter finds, in the institutionalist perspective, that electronic identity management policies are extending and stabilising the institution of data protection. IDM and e-ID policies reproduce core data protection principles and innovate with them in a new technical domain. This is accomplished through regulative and normative methods: laws, standards, value-laden

strategy documents, and, importantly, material technologies. As to the appearance of unlinkability in two separate polities, the technocratic nature of e-ID policy-making amplified the power of data protection practitioners who seized upon an opportunity to advance privacy regulations in their respective countries.

Policies of unlinkability further the institutionalisation of data protection, and materially embed its underlying principles. In line with institutionalist thought, policy decisions resulting in unlinkability were influenced by formal and informal mechanisms, and prior policy choices influenced later ones, engendering path dependence. US and German unlinkability requirements are isomorphic without having had direct, formal influence on one another. Coercive, normative and mimetic forces encouraged this isomorphism. Formal and informal relational networks of actors enabled the 'travel of ideas' (Scott, 2003, p. 887) among relevant policy stakeholders, carrying values and lexicons, enhancing the legitimacy of the strategy of unlinkability.

Material artefacts, such as the German e-ID card and the servers and applications of the US identity management 'ecosystem,' embed the values and preferences of policy actors, carrying and extending the institution of data protection. These artefacts are a durable expression of the institution, contribute to its stability, and evidence a re-application of core principles to recent technological developments. IDM and e-ID infrastructures are "crystallized institutions … both the outcome as well as the instruments of regulation" (Katzenbach, 2012, p. 130). In Germany, they embed a multi-decade policy commitment to the principles of proportionality, minimisation and context separation. In the United States, they represent the largest scale application to date of the Fair Information Practice Principles.

Digital identity is a product, subject to the institution of the market and its influences, as well as the prerogatives of e-government and data protection. It is a technology and a policy outcome, pregnant with multiple institutional influences and forces. New institutionalism treats technology as an analytic object, unearthing its submerged values. It shows how material objects, like the chip inside a German e-ID, move ideas "through space and time" (Scott, 2008, p. 79). This thesis contributes to institutionalist scholarship by subjecting the specific technologies of citizen credentialing to institutionalist analysis, testing it against rich empirical data.

Unlinkability architectures embed the underlying institutional forces of the policy domains they inhabit. These domains are suffused with the interests of many actors, and the policy outcome of unlinkability reflects the power of data protection practitioners. New institutionalism shows how regulative, normative and cultural-cognitive mechanisms work together to shape behaviour. This chapter explicates the above points, applying new institutionalist thinking to explain the similar outcomes in each country. Below are each of the propositions synthesised from the review of new institutionalism in Chapter 2. The propositions are applied to unlinkability, identity management and e-ID policy development in Germany and the US. This analysis highlights the cultural, structural, political, technological and economic forces that contributed to the emergence of unlinkability, enriching our understanding of information governance as a whole.

The choice to include unlinkability in citizen credentialing is influenced by formal and informal mechanisms.

Both the US and Germany had formal and informal mechanisms influencing the choice to include unlinkability in its credentialing efforts. The US Privacy

Act of 1974, a formal regulative instrument, was one of the laws applied to citizen credentialing. It states:

> "Each agency that maintains a system of records shall … maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency…." (Privacy Act of 1974, Sec. e(1))

This coercive requirement embodies the principles of proportionality and data minimisation. Unlinkable credentials reflect these principles by frustrating profiling activities, making it more difficult to identify citizens across varied online activities.

All US respondents cited the Fair Information Practice Principles as the key policy informing the privacy requirements for e-government credentials. The FIPPs are quasi-formal in that they are not binding law. Rather, they are a set of principles restated in various ways across a range of administrative documents and policies. The US National Strategy for Trusted Identities in Cyberspace, which applies to non-e-government credentials, explicitly bases its privacy rationale on the FIPPs, calling them "the widely accepted framework of defining principles to be used in the evaluation and consideration of systems, processes, or programs that affect individual privacy" (White House, 2011, p. 11). This language blurs the FIPPs' regulative and normative character. Their 'widely accepted' nature belies a "logic of appropriateness" (March and Olsen, 2004), yielding a "binding expectation" (Scott, 2008, p. 51) on policy actors. That expectation reinforces the inclusion of the FIPPs in formal policy instruments, creating a layer of data protection policy that does not exist as coherently elsewhere in federal law, as opposed to the formal data protection laws of Europe.

The US federal policy that directly affects the creation and management of citizen credentials for e-government access is the Trust Framework Provider

Adoption Process (ICAM, 2009d). Though the TFPAP requires 'minimalism,' its definition of that term does not encompass unlinkable credentials, stating:

> "Identity Provider must transmit only those attributes that were explicitly requested by the [relying party] application or required by the Federal profile." (ICAM, 2009d, p. 12)

The onus of data minimisation falls only on the relying parties and how they form their requests. Instead, it is the 'lower' levels of identity protocols and the technical specifications of the proposed Federal Credential Cloud Exchange that requires unlinkability in the most practical terms. Unlinkability was further supported by posts on an official identity management blog describing the federal government's wish to minimise 'panopticality' and discussions of the technical challenges therein (John, 2012). The term is not value-neutral: it connotes an all-seeing eye of far greater power than the subjects whom it observes (Reiman, 1995). Using such terminology is another method of legitimising unlinkability. Communicating the idea of panopticality in the context of identity management reinforces the value of data protection. Schmidt (2009, pp. 530-532) argues:

> "… political actors' ideas serve to (re)conceptualize interests and values as well as (re)shape institutions….[I]deas and discourse … help explain the dynamics of change (as well as continuity) in political economy."

By linking identity management discussions to the broader discourse of privacy, policy actors are engaging in a "coordinative discourse" and a "communicative discourse" (Schmidt, 2009, p. 531). Coordinative discourse involves "individuals and groups at the center of policy construction who are involved in the creation, elaboration, and justification of policy and programmatic ideas" (Schmidt, 2009, p. 531). Communicative discourse "consists of the individuals and groups at the center of political communication involved in the public presentation, deliberation, and legitimization of policy, programmatic, and philosophical ideas." (Schmidt, 2009, p. 531). The blog on

which panopticality is mentioned is meant for both identity management practitioners and the public at large. By using such language, the authors – one of which has been at the centre of US identity management privacy policy – build their case extending and innovating data protection in IDM.

Requirements to build credential systems that actively frustrate the profiling of citizens' online activity are value-laden and normative inasmuch as they are mandated by explicit regulative instruments; the formal and informal reinforce one another. The professionals and administrators responsible for creating technical and policy requirements for citizen credentialing interpreted formal laws and channelled the social expectations of data protection and privacy in the context of citizen use of the internet.

The entire US citizen identity strategy was influenced by a cultural rejection of national IDs. As one senior government administrator remarked:

> "… whenever you talked about a centralised organisation managing identities in the federal government, you come to national ID card, even if it's a virtual national ID card. You still end up there – somebody will raise that, and then everything dies when that happens, everything stops. (G001, Interview)

This constraint foreclosed the possibility of government-issued credentials, necessitating the involvement of private actors. The relatively weak data protection regime that could be applied to those actors caused federal administrators to innovate by extending the Privacy Act of 1974 to cover non-federal entities. This led to the 'comparability paradigm,' where private actors would need to show that their privacy and data protection mechanisms were at least comparable to federal ones. Many respondents took it for granted that a national identity scheme would be impossible to create in the United States (G001, Interview; G003, Interview; G007, Interview; G010, Interview; N005, Interview; N006, Interview; Thibeau, Interview). The belief is a form of orthodoxy. The highly influential 1973 Health, Education and Welfare report,

Records, Computers and the Rights of Citizens, which first codified the FIPPs in the US, spoke of the perception and potential harms of a "standard unique identifier" (SUI):

> "… the idea of an SUI is objectionable to many Americans.… Many people both feel a sense of alienation from their social institutions and resent the dehumanizing effects of a highly mechanized civilization. Every characteristic of an SUI heightens such emotions." (U.S. Department of Health, Education and Welfare, 1973, Sec. VII)

The data under study shows this view to be alive and well. One privacy advocate noted:

> "… when you say 'national ID card' or 'national ID card for the internet,' people's instinct is to go for repression and no privacy. That's what resonates in people's heads." (N005, Interview)

Correspondingly, the 2011 National Strategy for Trusted Identities in Cyberspace states:

> "… the Strategy does not advocate for the establishment of a national identification card or system." (White House, 2011, p. 8)

The culturally supported, common belief that the American people reject national identity systems locked policy-makers into the need to obtain credentials from private sources. This caused them to embrace the institutional influences of the market and higher education in order to find suppliers. These private actors have so far lacked incentive to supply citizens with high assurance credentials – a strong enough business case to justify the investment is yet to materialise. Had the US government been able to supply its own credentials, like Germany, its exposure to market forces would be limited with respect to e-government authentication. The government perceives a higher value to citizen credentials than private organisations. This illustrates the institutional conflict at work in citizen credentialing. The state, paternalistically setting privacy policy for its citizens to reduce potential harms of profiling and 'unfair' information practices, required citizen credentials from private actors

to conform to federal privacy policies that the actors would otherwise not be subject to. The private actors were willing to meet these requirements, but not without remuneration to build the complex systems citizen credentialing entailed. Government could pay for those credentials, but has so far declined to do so. The needs of government and the market are orthogonal to one another, and have not aligned sufficiently to achieve the government's goals of enabling strongly authenticated, privacy-preserving e-government access. This highlights "how institutions mediate and filter politics" (Thelen and Steinmo, 1992, p. 16). At present, only one university and no private companies are offering FICAM-compliant credentials for general use by the citizenry.

Germany shows similar formal and informal mechanisms at work in the choice to enable unlinkable credentials. Unlike the US, Germany has a general data protection law, which is a transposition of the supranational EU Data Protection Directive. Section 3a of the German Federal Data Protection Act (2003) states:

> "Personal data are to be collected, processed and used, and processing systems are to be designed in accordance with the aim of collecting, processing and using as little personal data as possible. In particular, personal data are to be aliased or rendered anonymous as far as possible and the effort involved is reasonable in relation to the desired level of protection."

The 1983 Constitutional Court decision also acts as a formal constraint over the treatment of personal data. It derived a right to informational self-determination from the German constitution, and forbade the state from being treated as a single data processor (Hornung and Schnabel, 2009). The *Personalausweisgesetz*, the law establishing the e-ID card and most of its privacy features, co-exists with the court decision and data protection law. The pseudonymity features of the e-ID exist as official technical specifications from the Federal Office for Information Security (2011). The procedures for becoming authorised to access the e-ID and to interact with the card

pseudonyms are published by the Federal Office of Administration. The competency for identity documents is established by law at the federal level, but citizen registration is legally specified at the state level (ULD, Interview). Each state has a data protection authority, responsible for the data protection of the civilian registries.

There is no requirement for the Ministry of Interior to consult the state data protection authorities (ULD, Interview). However, the Ministry did consult them for their expertise and to encourage them to support the decision to deploy an e-ID (ULD, Interview). Marit Hansen, the Deputy Privacy & Information Commissioner of Schleswig-Holstein, observed, "it is always good to talk to Data Protection Authorities if you want acceptance" (ULD, Interview). The pseudonymity function of the e-ID was directly influenced by this informal inclusion of the views of the state authorities. Pseudonymity was a part of the data protection landscape, enshrined in both a telecommunications law and an earlier e-signature law (ULD, Interview). The normative value of pseudonymity, data minimisation and context separation 'travelled' from the data protection authorities to the Ministry of Interior. Marit Hansen noted:

> "… if everything is more digital and you want more acceptance also from the Data Protection Authorities, you should always have the possibility of pseudonym function…." (ULD, Interview)

There is a taken-for-granted quality to the policy of unlinkability.

In both the German and US case data, respondents relate views that represent cultural-cognitive carriers of institutionalised data protection. In Germany, a privacy mindset is cited (DE-G003, Interview; Möller, Interview; ULD, Interview). Of the origin of the unlinkability requirement, one engineer said there was "not a specific service or application behind it, it was more … a general approach following, let's say, a common mindset...." (DE-G003,

Interview). Jan Möller noted that pervasive cultural issues around privacy were the backdrop of the e-ID:

> "… privacy and self-determination, it's a big issue in Germany. Basically the whole privacy issue is something [that] has had a lot of cultural background and how you feel about it and what do you think, what is private and what is not private." (Möller, Interview)

Jens Fromm, a scientist at the Fraunhofer research institution, explained in cultural terms his preference for a state-issued form of ID over commercially-derived ones:

> "… in some situations, I am strongly convinced that it's good that we have a sovereign state-given identity…. This is not something I can *rationally* explain. I think this is really a cultural and somehow philosophical question.…" (Fromm, Interview)

In the US, the identity management expert, Paul Trevithick (Interview) spoke of a design ethos among technologists:

> "… we believe in this stuff and want to do this stuff.… We get up in the morning and we think about distributed systems, we think about anti-centralisation whatever, we try to shift control out to the edge of networks and … I think we all have this natural feeling, like, shouldn't we be sovereign actors, and shouldn't information about us be … as much as possible under our fingertips and controls?"

A senior US government official spoke of her belief in a right to anonymity:

> "I think, certainly in common law countries, where much of this body of regulation grew from, we have a belief – an underlying principle – that people should have some right to anonymity." (G001, Interview)

The National Strategy for Trusted Identities in Cyberspace cites the 'vital' requirement of pseudonymity:

> "It is vital to maintain the capacity for anonymity and pseudonymity in Internet transactions in order to enhance individuals' privacy and otherwise support civil liberties." (White House, 2011, p. 1)

In Scott's pillars of institutions (2008, p. 51), the above citations are understood as common beliefs, orthodoxy and shared logics of action. They mesh with normative and regulative elements of data protection. The NSTIC quote is 'communicative discourse,' using language and ideas to involve the public in considerations of privacy within identity management (Schmidt, 2009). One US identity management policy administrator stated, "the work that we're doing is focussed very much on doing the right thing by our citizens in protecting … any services that we deploy that are citizen-facing" (G009, Interview). Unlinkable credentials and other privacy-preserving requirements are the rules and artefacts of what is 'right.' The ethos of designers is made more durable in the form of standards and the technologies that rely upon them. The German privacy mindset is fixed in regulative laws and the cryptographic design of the e-ID. *There is no discrete boundary between the culture of privacy, the laws that require it and the technologies that fix it in hardware.*

Values embedded in material technologies can encourage people to take their presence and underlying principles for granted. The 'rules-in-use' – the actual use of institutional rules by those subject to them (Ostrom 1992, p. 19) – here are citizens using e-IDs and private credentials to access various websites. Awareness of their privacy-preserving characteristics and repeated use of them can cause citizens to believe in their appropriateness, reinforcing the views of the policy-makers, strengthening the overarching institution. In this way, identity technologies frame online interaction

> "… through the infrastructure they provide and the negotiated or established uses attached to it. In this sense, they are 'taken-for-granted,' a more-or-less invisible and untested background and frame for social structures and our daily courses of action." (Katzenbach, 2012, p. 130)

And indeed they are invisible to users. The cryptographic processes performed by the German e-ID or the proposed US FCCX are abstract and imperceptible

to the citizens they serve. That invisibility, claims Pinch (2008, p. 467) enhances the power of the material dimension of data protection:

> "It is because social choices appear to have vanished from technologies, or are so deeply embedded within technical structures that they become invisible to all but the technical experts, that technologies are powerful institutions."

Invisibility is a hallmark of the internet – its ubiquitous use derives in part from hiding its complexity. As more people use the internet, the institutions embedded within its architecture will see further enactment. However, that architecture is pregnant with many institutions – data protection, the market, law enforcement, government – overlapping and sometimes in direct conflict. In this we see Lessig's (2006; see also Koops and Leenes, 2005) 'code is law' argument modulated by competing institutional effects. The invisible architecture of the internet is as much a battleground for competing institutions as it is for competing code.

There is an isomorphic dimension to the choice to require unlinkability.

Despite their differences in policy history, culture and technology, both Germany and the United States – as well as other nations such as Canada and Austria – have enacted policy requiring various forms of unlinkability. This 'homogenisation' reflects DiMaggio and Powell's (1983) view that coercive and normative mechanisms cause organisations to become isomorphic with one another. Of coercive isomorphism, they write:

> "Coercive isomorphism results from both formal and informal pressures exerted on organizations by other organizations upon which they are dependent and by cultural expectations in the society within which organizations function. Such pressures may be felt as force, as persuasion, or as invitations to join in collusion." (1983, p. 150)

And, of normative pressures, DiMaggio and Powell write:

> "A … source of isomorphic organizational change is normative and stems primarily from professionalization.… we interpret professionalization as the collective struggle of members of an occupation to define the conditions and methods of their work, to control 'the production of producers' … and to establish a cognitive base and legitimation for their occupational autonomy…." (1983, p. 152)

Both US and German data protection policies have similar principles at their core. They are also enacting unlinkability mechanisms in the same timeframe as one another. Without direct policy influence between them, it is fruitful to consider which isomorphic forces may be influential.

As Gellman has shown (2012), the Fair Information Practice Principles have existed in some form since the early 1970s. The substance of those principles appears in the Privacy Act of 1974, the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, the 1995 EU Data Protection Directive, the 2003 German Federal Data Protection Act, FICAM's privacy requirements, and the National Strategies for Trusted Identities in Cyberspace (Gellman, 2012). In 1972, a British Parliamentary committee on privacy wrote that "[t]he amount of information collected and held should be the minimum necessary for the achievement of the specified purpose" (Gellman, 2012, p. 3). This principle of minimum disclosure, early in the history of data protection, has been restated in a variety of forms in the instruments outlined above and continues to exert influence on policy actors. Unlinkability is a direct expression of this principle, and its presence in German and US policy reflects both coercive and normative influences on policy-makers. In Germany, the coercive force is more evident as the minimum disclosure principle is codified in federal data protection law. In the US, the coercive nature of the minimum disclosure principle is more informal – though still potent – because of a lack of an omnibus data protection policy that includes the principle. Minimum disclosure is a strong value within the data protection community of practice, as evidenced by its consistent inclusion in

policy instruments for over 40 years. The reproduction of minimum disclosure, collection and use limitation, proportionality, purpose specificity and a respect for context separation are, as DiMaggio and Powell (1983, p. 152) note above, part of this professional community's "collective struggle … to control 'the production of the producers'…."

Standards are another site of isomorphic influence, encompassing regulative and normative elements. Pinch (2008, p. 472) writes:

> "Standards are rarely simple technical matters; they are powerful ways of bringing a resolution to debates that might encompass different social meanings of a technology. Standards are set to be followed; they entail routinized social actions and are in effect a form of institutionalization."

In Scott's terms (2008, p. 79), standards are routines, carrying the regulative elements of institutions, though given their technical nature can also be seen as artefacts. Identity management and data protection rely on a panoply of standards. SAML 2.0 had a sufficient capability to produce unlinkable credentials but OpenID 2.0 did not, and had to be altered during the course of FICAM's policy development to meet government specifications (N003, Interview). SAML has the ability to issue a new (ephemeral) pseudonym each time an identity provider communicates with the same relying party as well as the ability to issue the same (persistent) pseudonym to the same rely party for each return visit. The specification designers felt that the ephemeral pseudonym was a valuable privacy-preserving feature, but it has seen no use (N003, Interview). One senior standards developer explained:

> "It's not supported in very many products and probably would just cause things to blow up. So it's one of those things that when we were creating SAML seemed like a good idea but never got any deployment…. In general, people use federated login to identify people over time ... doing a single SAML authentication with a bunch of claims that let you do something like an 'over-eighteen claim' … but … prevented the relying party from telling that you are the same person

> who came last time … it's a theoretical problem and has no real world uptake, at least with SAML." (N003, Interview)

Standards development organisations and their human members are institutional actors, and the standards they publish are carriers of institutionalisation. In this case, data protection is innovating with regard to the advent of identity management technologies, and standards developers have encoded their values into relevant specifications. This institutional development has been embraced in the persistent pseudonym case, but not in the ephemeral case. The logic of the market – here, lack of take-up due to lack of demand – is in tension with the ethos of the SAML specification writers. However, the specification exists; it is durable. Products based on SAML are not neutral; they contain the values of the specification writers. Should the market case for ephemeral pseudonyms improve, the normatively-infused specification can affect the data protection characteristics of new products. The values of standards developers 'travel' through the standards they define. Like data protection practitioners, standards developers are professionals who influence "the production of producers" (DiMaggio and Powell, 1983, p. 152). If Galloway (2004, p. 122) is to be believed,

> "… this loose consortium of decision makers tends to fall into a relatively homogenous social class: highly educated, altruistic, liberal-minded science professionals from modernized societies around the globe."

Galloway supplies no methodological evidence for this claim, but despite this, it reflects the more defensible position that standards are inescapably political. As Kapor (2006) observed, "architecture is politics."

International standards defining unlinkability and related privacy configurations have been in development for several years. Standards committees are thereby an important site of isomorphism. A workgroup of the International Standards Organization (ISO) is developing IEC/ISO 29191,

"Requirements for partially anonymous, partially unlinkable authentication" (De Soete, 2013). This workgroup, WG5, falls under the ISO's Joint Technical Committee 1 / Subcommittee 27 (JTC1/SC27), whose membership includes representatives from 50 countries. The committee is led by Dr. Walter Fumy, co-editor of a book on e-ID security that features the German e-ID as a prominent case study (Fumy and Paeschke, 2011). SC27 is a relational network for professionals and other stakeholders to exchange ideas and values, ultimately returning to their home countries and organisations with explicit documentation and the invisible narratives that will inform their work.

SC27 published a terminology document that "serves as a basis for desirable additional privacy standardization initiatives, for example a technical reference architecture, the use of specific privacy technologies, an overall privacy management, assurance of privacy compliance for outsourced data processes, privacy impact assessments and engineering specifications" (Rannenberg, Sténuit, Yamada and Weiss, 2007). As another form of isomorphism, this normative lexicon helps to shape and legitimise the privacy views and subsequent actions of data protection practitioners, scientists, product managers and the many other stakeholders in identity management. Meyer and Rowan (1977, p. 349) called this a 'vocabulary of structure':

> "From an institutional perspective, a most important aspect of isomorphism with environmental institutions is the evolution of organizational language. The labels of the organization chart as well as the vocabulary used to delineate organizational goals, procedures, and policies are analogous to the vocabularies of motive used to account for the activities of individuals…. Vocabularies of structure which are isomorphic with institutional rules provide prudent, rational, and legitimate accounts." (Meyer and Rowan, 1977, p. 349)

SC27's lexicon carries the institution of data protection, evolving it, rationalising newer privacy-preserving strategies like unlinkability. Similar efforts to legitimise privacy in identity managment are visible in other fields, such as academia and government research. Marit Hansen of the ULD

collaborated with Andreas Pfitzmann (2010) of the Dresden University of Technology on "A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management," which attempts to define key privacy terms and translate them into 10 different languages. The eGovernment unit of the European Commission funded the Modinis-IDM project which published a Study on Identity Management to "progress towards a coherent approach in electronic identity management in eGovernment in the European Union" (Modinis IDM Study Team, 2005). This Study contained a "Common Terminological Framework for Interoperable Electronic Identity Management" as well as a set of identified 'good practices.' More expansive was the Future of Identity in the Information Society (FIDIS) project funded by the European Union which produced an extensive body of research on the technical, conceptual, social, law enforcement, legal and economic dimensions of digital identity (Rannenberg, Royer and Deuker, 2009). These lexicons, standards and research reports are a rich repository of language, values, narratives and technical designs that 'travel' and are reproduced throughout the world of identity management. Privacy norms and material possibilities are thus transmitted, providing a partial explanation for the developement of unlinkability in different polities.

Prior policy choices constrained and affected the choice to require unlinkability.

In Germany, the decision of the 1983 Constitutional Court looms large over all data protection policy subsequent to it. The right to informational self-determination – the "legal anchor for data protection in the German constitution," (Hornung and Schnabel, 2009, p. 84) – the principles of proportionality and data minimisation, and the banning of the state being treated as a single data processor were the backbone of the privacy architecture

of the e-ID system. The power of the German court and its long-lasting effects contribute to the stability of the institution of data protection, supporting the evolutionary step of fixing unlinkability in the architecture of the e-ID. The court decision itself was dependent on the creation of a new German constitution in 1949. The rights to dignity and the full development of one's personality, enshrined in the first two articles, are directly responsible for the legal reasoning allowing the court to derive the informational self-determination right (Rouvroy and Poullet, 2012).

The course of German policy was also influenced by its membership in the European Union, which required the transposition of EU directives into national law. Consequently, German data protection policy is modelled on the 1995 EU Data Protection Directive which contains the principle of proportionality. German policy choices were also dependent on the historical requirement to possess an identity document, dating at least from 1938 (Noack and Kubicek, 2010, p. 93). National identity cards are institutionalised in Germany, and the introduction of an electronic ID to replace the laminated paper one is a 'path continuation' (Noack and Kubicek, 2010, p. 107). Merged with this path is the e-passport. The e-passport infrastructure pre-dates the e-ID, though engineers and policy-makers were contemplating an e-ID when designing its architecture. One senior scientist recalled:

> "… when we started designing the protocols for the e-passport we already had also an identity card in mind. So when we planned for the protocols we planned it in a way we could also base an identity card on [it]." (DE-G001, Interview)

Noack and Kubicek (2010, pp. 107-110) note that the authorisation process needed to access the e-ID card data and resultant technical certificates are a 'path creation':

> "There is no predecessor for a similar certification procedure for online access to personal data in other sectors in Germany or anywhere else in the world." (Noack and Kubicek, 2010, pp. 107-108)

The e-ID's pseudonym capability, however, can be seen as a path continuation. A 2007 telecommunications law requires internet services to enable pseudonymous use where possible:

> "The service provider must enable the use of telemedia and payment for them to occur anonymously or via a pseudonym where this is technically possible and reasonable." (Telemedia Act, Sec. 13(6))

The Federal Data Protection Act also sets a bias for pseudonymity ('aliasing'):

> "Personal data are to be collected, processed and used, and processing systems are to be designed in accordance with the aim of collecting, processing and using as little personal data as possible. In particular, personal data are to be aliased or rendered anonymous as far as possible and the effort involved is reasonable in relation to the desired level of protection." (Federal Data Protection Act, 2003, Sec. 3a)

Unlinkability can thereby trace much of its policy influences to these earlier laws. The pseudonymity requirements of the Telemedia Act and the Federal Data Protection Act are given specific effect in the pseudonymity function of the e-ID.

In the US, the influence of prior policy choices is more diffuse. The Fair Information Practice Principles are not binding law, though they are the strongest influence on the choice to require unlinkability. The FIPPs inform the Privacy Act of 1974, which exerts influence on the privacy requirements for citizen credentialing for e-government, although the FIPPs themselves are cited as the core principles at work (G001, Interview; G003, Interview; G006, Interview; N005, Interview). In the NSTIC, a 2008 formulation of the FIPPs is cited explicitly as the grounding principles for privacy in the 'identity ecosystem' for non-e-government credentials (White House, 2011, p. 12). One legal researcher noted that this use of the FIPPs is the first omnibus application of it in the US (Dazza Greenwood, Interview). Unlinkability embodies the FIPPs' data minimisation principle, reflecting and reinforcing, as in the

German case, the institutional stability of data protection and its capacity to adapt to new technical developments.

Pseudonymous access to government services was envisioned in the US Electronic Authentication Partnership, an evolutionary precursor to FICAM. Though intended for low assurance transactions, where little or no confidence in a claimed identity is needed, identity management policy-makers and government consultants incorporated the view that "less is more" (P006, Interview). Chris Louden, one of the security and privacy consultants involved in the EAP, and his associates continued to consult on later identity management policy. He and his associates co-authored FICAM's identity schemes and contributed to FICAM's general privacy framework (N003, Interview; P006, Interview; Wilsher, Interview). This continuity of actors contributed to a continuity of values in the development of IDM policy.

Where Germany had pre-existing identity document requirements, the absence of such requirements and the strong antipathy towards such policy forced the US to engage private actors to fulfil its policy goals. The spectre of a national ID and the political difficulties of government-supplied online credentials caused the US to go down a path that implied cooperation with private organisations, effectively necessitating multi-stakeholder governance. This path forced the commingling of government and market needs. Government institutional logic can mandate particular privacy requirements in service of societal privacy goals. Market logic, however, need not share these goals, and in the absence of mandatory legal requirements, is not necessarily aligned with government. Further, market actors need compelling reasons to spend money on system development and operation. By comparison, Germany did not need the complicity of the market to deploy e-ID cards: it created policy, bought the infrastructure, and distributed the cards. Due to the orthogonal interests and

logics of the government and private industry, citizen digital identities in the US are stalled.

US and German citizen IDM efforts both follow initial forays into e-government. The data shows that e-government is a driver of identity management, though not exclusively. This finding is consistent with prior research on IDM in Europe (Kubicek and Noack, 2010). The need to exchange personal data in citizen-government interactions in combination with the difficulty of authenticating people on the internet contributed to greater policy activity around citizen digital identities, which ultimately contributed to privacy and data protection policy changes. In the US, the choice to require unlinkability comes from a reapplication of pre-existing privacy principles by administrators, consultants and privacy professionals. In Germany, e-government and other forces drove the federal government towards the replacement of their paper identity card with an electronic one. The seminal Constitutional Court case nearly 25 years prior exerted a strong influence on the choice to include unlinkability as a feature of the e-ID system.

Both the US and German case data show effects from the terrorist attacks of 11 September, 2001, which could be construed as an 'exogenous shock' or 'critical juncture.' In the US, this event triggered a spate of cybersecurity activity in government, influencing the development of US identity management policy. One senior government official recalled, "there were a lot of them that came out that time, a lot of homeland security presidential directives, but they were all responses to the report that came out on 9/11" (G001, Interview). A different government official, however, did not see September 11th as a policy driver (G003, Interview). That said, the decision to include unlinkability does not appear to be influenced directly by the event. Rather, the policy environment reflected a heightened focus on security

generally, and in the domain of information sharing specifically. Another government official said that

> "… the issue of information sharing is significant for the federal government. Not just because of post-9/11, but certainly because of post-9/11…." (G006, Interview)

In Germany, two electronic identity scholars both saw the 9/11 attacks as influential on e-ID policy development (Noack and Kubicek, 2010; Hornung, Interview). However, this influence seemed to extend only to questions of the inclusion of biometrics – again, a security issue rather than privacy. As in the US case, the terrorist attacks were influential on the general policy milieu rather than on privacy choices within identity management. Gerrit Hornung (Interview) observed:

> "… after September 11, people in Europe started to think about having this biometric passport … the German biometric passport started in 2007 … and so when people started to implement that project I think there were parallel thoughts on having biometric data on the identity card as well, and obviously that implied changing the technical base of the identity card because the former one didn't have a chip. And so that was definitely one thing where the actual project … got momentum from because then obviously people from the more e-government-oriented side started to think, 'Okay, if we change the technical base of the whole thing anyway, so why don't we then provide e-government applications by the new identity card as well?'"

Institutionalist scholarship argues that historical events, timing and sequence affect policy outcomes. In the empirical data, there is an oblique effect of the terrorist attacks of September 11th. More potent is the sequence of policies. In both cases, e-government policy commitments predate and strongly influence identity management and its privacy elements. In Germany, the e-ID is based on both the prior national identity card and the predating e-passport.

Networks of social actors influenced the policy of unlinkability.

One of Scott's (2003, p. 886) four 'carriers of institutionalisation' is "relational systems," which are "made up of connections among actors, including both individual and collective actors." These systems are networks that "connect organizational decision-makers … through professional and business associations and interlocking memberships" (Scott, 2003, p. 887). Identity management, data protection and privacy professionals interact in such networks, diffusing ideas between themselves over time and geography.

Organisationally and individually, the US identity management community has had a diverse and often consistent group of actors since the late 1990s. Some of the same government officials involved in developing President Bush's E-Government identity management initiatives continued to shape policy in the Electronic Authentication Partnership and FICAM (G003, Interview; G004, Interview). Technologists who developed novel identity management technologies sat on a variety of IDM standards committees and contributed to policy development (Trevithick, Interview; Reed, Interview; P001, Interview). Businesses and individuals involved in standards development work ultimately saw their efforts incorporated into Trust Framework operators, such as the Kantara Initiative (Nash, Interview). Those efforts were also then submitted to international bodies to become incorporated into global standards (Wilsher, Interview). Government privacy lawyers involved in FICAM were also authors of the privacy language in the NSTIC and privacy policy at the Department of Homeland Security (G006, Interview; G010, Interview). Individuals from government and industry sit on international standards working groups (N003, Interview; P001, Interview). These interlocking sets of relationships – these 'communities of practice' – foster the "travel of ideas" (Scott, 2003, p. 887). From informal discussions in hotel lobbies to the durable encoding of views and values in open standards and proprietary technologies, these networks facilitate isomorphism and the diffusion of policy preferences. In this way, the

normative views of consultants, engineers, policy-makers, advocates and business managers proliferate and are reified. This helps to explain the appearance of unlinkability across a range of countries.

In the case of Germany, there are a variety of interlocking relationships. As Marit Hansen (ULD, Interview) noted in Chapter 6, the Ministry of Interior engaged state data protection authorities for their expert views. There was much interaction between the Ministry and its sub-agencies, the Federal Office for Information Security (BSI) and the Federal Office of Administration (BVA). During the e-ID's policy development, the Ministry and the German Parliament communicated extensively, with input from the Federal Commissioner for Data Protection (ULD, Interview). To develop the certification regime to access e-ID card data, the BVA convened working groups comprised of Ministry representatives, the BSI, and industry (DE-G002, Interview). Technical specifications were designed by the BSI working in concert with the German Industry Forum and an IT industry association, BITKOM, whose members included card manufacturers, chip manufacturers, Microsoft, T-Systems, and the German Federal Printer (Noack and Kubicek, 2010, pp. 103-104). The ULD, one of Germany's leading data protection authorities, has been involved in a number of European projects that connected them to a much larger, international community of practice (ABC4Trust, 2012; FIDIS, n.d., FutureID, n.d.; PrimeLife, n.d.). Members of the ULD also worked directly with data protection and identity management academics, producing substantial peer-reviewed work. European projects such as ABC4Trust brought together scholars, data protection authorities and technology companies such as IBM and Nokia-Siemens Networks (ABC4Trust, 2012). All of these interlocking relationships foster formal and informal connections among participants, institutionalising data protection through shared values and requirements encoded into standards and technologies. Claus Offe (2006, p. 16) writes:

> "Institutions are dependent upon requisite sectoral virtues and informal codes of conduct.… No institution can function unless such corresponding informal codes of conduct and sector-specific ethos are observed by participants. One important function of institutions is to inculcate such loyalty."

Through professional connections, the 'sectoral virtues' of data protection – which include a bias against profiling – are transmitted. Scott (2003, p. 890) calls this "combined carriers":

> "Relational ties provide the conduits, but cultural beliefs supply the content."

In some of his most recent work on institutions, Scott (2003, pp. 888-889; 2010, pp. 13-14) highlights the importance of intermediaries:

> "To the categories of producers and users of ideas must be added a collection of go-betweens – intermediaries that do not create but transmit and market information." (2003, p. 888)

> "… [a] broad collection of actors [who] help to enable and guide action and, more generally, serves to 'thicken' and stabilize the fields in which they work." (2010, p. 13)

These intermediaries are clearly visible in the US case in the form of the Trust Framework Providers: the OIX, Kantara, SAFE-Biopharma and InCommon. The organisations seek to broker relationships on behalf of their members and clients. With regard to data protection, they behave differently depending on their stakeholders. The OIX was effectively neutral with regard to the government's credential requirements, passing their requirements intact to the participating entities (Thibeau, Interview). InCommon, however, took a more active role, negotiating directly with the government when it saw the requirements as misaligned with its educational members' needs (Morgan, Interview). In all cases, the TFPs must accredit auditors who then certify that applicant organisations meet the government's requirements. The

government's requirements are 'translated' by the TFPs into language that the assessors can use in their assessment. In this way, the TFPs 'stabilise' the market for citizen identities, in Scott's language, and become a site of power exchange between stakeholders and intermediaries.

Pinch (2008, pp. 476-477) also highlights the importance of intermediaries, specifically salespeople:

> "In building markets, a key part is played by mediators like salespeople. It is salespeople who move between the world of use and the world of design and manufacture and who bring the two into alignment. We need to pay more attention to intermediaries such as salespeople and repair people."

One of the challenges facing the German e-ID is weak marketing. A Fraunhofer scientist observed:

> "I think [what's] crucial really is … the marketing aspects. Why should citizens use the identity function, are they aware of these identity functions? About 65% of the citizens are opting out the function because they just don't know why they should use it, why they should opt in." (Fromm, Interview)

As of February 2013, 72% of citizens were opting out, turning off their e-ID's online authentication functions (Bundesverwaltungsamt, 2013). This marketing weakness hampers policy-makers' intentions to make the e-ID broadly usable with commercial and e-government services. Commercial organisations are largely unconvinced of the value of becoming certified to access the card data, and municipality staff and citizens are not aware of the value of using the card online (DE-G002, Interview). Members of the Federal Office of Administration (BVA) spend a significant amount of time traveling around Germany trying to convince organisations and people of the e-ID's value. One official noted:

> "We also want to win clients to … use this function. Of course we're doing also a little bit of promotion for this. Germany has invested a lot

> in this so we want companies and Government to use it.... We initiate conferences, we go to the states, we go to the cities, we talk to them and inform them about the possibilities and the functions that they could use just so that they get an idea of what they can benefit from.... Like a product convention." (DE-G002, Interview)

In this way, BVA staff is an active part of the adoption of the e-ID's privacy features. The selective disclosure of age and locality and the pseudonymity function, elements that innovate the institution data protection, have to be used to become part of the landscape. In their role as salespeople, the BVA staff is a conduit, building the 'market' for digital identity interactions. They align the policy goals of informational self-determination and trustworthy online transactions with the realities of deploying an e-ID 'product.' The municipal office staffs can be viewed as underutilised salespeople. By not supporting them with more information, or including them in the communicative discourse of the value of the online authentication feature, the BVA turned potential allies into neutral or hostile parties.

Identity management is complex technologically, politically and in regards to business relationships. US policy documents speak of an 'identity ecosystem,' (White House, 2011) highlighting the interconnected nature of various actors. This ecosystem is made of businesses, governments, standards and their development organisations, advocates, products, markets, political arrangements and the public. Information policy-making within this ecosystem is iterative and collaborative, involving public and private actors alike. This complexity and diversity complicates policy-making, implementation and enforcement, necessitating multi-stakeholder governance. On this point, Katzenbach (2012, p. 120) writes:

> "Due to the increasing complexities, dynamics and diversity of contemporary societies and their communication structures, the efficacy of statutory regulation is seen as limited; therefore, private actors are included in regulative structures."

Within the US case, this is best exemplified by the use of Trust Framework Providers to assess private identity providers for comparable privacy and data protection policies. The TFPs are private organisations and, as discussed above, are sometimes neutral and sometimes not. Privacy goals are filtered through the TFPs because the US government has elected not to issue its own identity credentials. The policy domain of identity management, influenced by the institution of data protection, is pregnant with a variety of interests. The complexity of identity management invites compromise, the translation of goals, and mutualism in order to advance. Trust Framework Providers are relational as well as symbolic systems, composed of networks of actors and governing rules. They are "both the outcome as well as the instruments of regulation" (Katzenbach, 2012, p. 130)

Material artefacts further institutionalise data protection.

Unlinkability is a characteristic of a technical system. The chips, servers and code that render credentials unlinkable are a material embodiment of data protection and privacy values and choices. The German e-ID system relies on cryptographic functions embedded within its authentication architecture to create unlinkable pseudonymous logins. The unobservable characteristic of the e-ID system as a whole, denying the government information about citizens' online activities, derives from an architecture that specifically eschews centralised servers. These technical features are not by-products – they are intentional choices writ in code and silicon, reflecting the norms of actors and their communities.

Though it lacks an identity card-based infrastructure, the US system is similarly value-laden. The use of servers and applications configured to create pseudonyms on a per-relying party basis, and the architecture of the proposed Federal Cloud Credential Exchange, designed to blind both relying parties and identity providers, are material reifications of data protection values and policy

choices. The appearance of the term ‘panopticality’ on official blogs (Gallagher and Lefkovitz, 2012) connects US data protection to the broader discourse of privacy research. The technology of the FCCX seeks to diminish such omnipresent monitoring, materially embedding the values that deem panopticality harmful and unfair.

As technology changes, so must the institution of data protection. Lowndes (2010, p. 66) observes that institutions are changed and sustained though human action. The use of federated identity technologies and cryptographic identity cards require data protection practitioners to actively reapply and reinterpret institutional logic. In the case data, this happens via multiple carriers: new laws, new networks, changes in standards, and new technologies. The principles of data minimisation, proportionality, context separation and a bias against profiling are interpreted and filtered through actors, ‘localising’ the regulative, normative and cultural-cognitive elements of data protection. As DiMaggio observes:

> “… central institutional forms will be subject to local modification. Such local modifications represent a pool of potential innovations that may themselves diffuse to organizations throughout the field.” (DiMaggio, 1988, p. 15)

The pseudonymity generator on the German e-ID and the unlinkable design of the FCCX are part of this pool of innovations, and both have the potential to diffuse through the field of identity management through its various organisations and actors. Both sets of technology anchor the locally interpreted institution in a self-reproducing material dimension. They stabilise the institutional innovation of unlinkability, and further institutionalise data protection within society. In the German case, the e-ID is a multi-decade commitment to the normative and legal principles underpinning national data protection and privacy priorities. In the US, the FCCX is a pilot project, trialling the various and complex components needed for a privacy preserving

'identity ecosystem.' Both of these technologies are also technical forms of enforcement; ostensible improvements on a reliance on purely social methods of administering privacy requirements. They add to the 'mosaic of solutions' to regulatory problems (Bennett and Raab, 2003, p. 165).

Identity management is a combination of "the technical, political, social, and economic" (Pinch, 2008, p. 468). Institutional forces strongly influenced the inclusion of unlinkability in the design of US and German identity management systems. In the German case, the weight of cultural privacy imperatives, and the normative and regulative force of the 1983 Constitutional Court case urged the e-ID design towards one that would reinforce informational self-determination. The interpretation of that right influenced Jan Möller and his colleagues to build in a capability for unlinkable logins. In America, the technological innovation of the FCCX afforded an opportunity for the institutional innovation of enforcing unlinkability technologically on non-governmental actors, extending central features of data protection without additional legislation. In both cases, institutional innovation was possible because of the power of the data protection community in each country, augmented by the technocratic nature of electronic identification policy. That power is reflected in the durability of the technical artefacts of unlinkability.

The requirement of unlinkability embeds the power dynamics of actors and institutional relationships.

Unlinkability is institutional development (Jepperson, 1991), extending and reapplying core data protection principles within a new technical milieu. It comports with Jepperson's (1991, p. 152) description:

> "Institutional development (or elaboration) represents institutional continuation rather than an exit – a change within an institutional form."

Its appearance in the information policy of Germany and the US is evolutionary, and illustrates growth of the power of certain institutional actors. Levi (1990, p. 407) observes:

> "Some institutions serve the interests of the many, some the interests of the few, but all facilitate and regulate resources of power."

The institution of data protection serves the interests of the many – human data subjects. The strength or weakness of the institution influences how much power is accorded its practitioners and their capability to enforce the norms of data protection. Requirements for unlinkability in citizen credentialing are an exercise of the power of data protection policy-makers and advocates in a world of fast-evolving technology.

Data protection is well-institutionalised in Germany. Burkert (2012, p. 101; see also Noack and Kubicek, 2010, p. 95) notes that the German state of Hesse created the world's first data protection law in 1970. German history, its adherence to EU law, privacy mindset, extensive system of data protection authorities (DPAs), and strong academic focus on privacy and data protection all contribute to this well-institutionalised character. The strength of state data protection authorities, for example, helps explain why the Ministry of Interior included them in policy development even though they were not formally required to do so. That inclusion also demonstrates the need for technical expertise during policy considerations of electronic identity issues. The technocratic nature of e-ID policy-making amplified the power of the authorities. The ULD, in particular, led the state DPAs' input to the e-ID policy process because they had been involved in a number of pan-European electronic identity research projects (ULD, Interview). Jan Möller, after he was hired away from the ULD to the Ministry, was given wide latitude to develop the privacy architectures of the e-ID card. Herbert Kubicek noted:

> "… [they] hired Möller to take care of the privacy issues. And my impression is that they didn't really care what he proposed because they

> believed in him, because the ULD is the most critical of all sixteen privacy state offices. So if they agree with something, you can be safe that there will be no discussion following…. [I]t was his idea to bring in this [pseudonymity] function which is contrafactual to what the main project was about…. the ULD just had finished a huge project on unobservability and unlinkability…. So out of this experience and this project he just had it in his head and he was free to… nobody cared to stop him or ask more." (Kubicek, Interview)

Discussions of the pseudonymity and selective disclosure features did not rise to the level of Parliamentary debate (Hornung, Interview; Kubicek, Interview). The only data protection concerns to reach that level were the inclusion of biometrics and the question of centralised databases. Gerrit Hornung, recalled:

> "… political debate on this new identity card I believe focused to, say, 90% on that biometric issue, so neither the electronic signature function nor the authentication mechanism or the pseudonym function … played a major role in the political debate. That was possibly in part due to the statements of … data protection officers. I mean the federal data officer made a strong claim against the fingerprints, but on the authentication mechanism, he said, 'Well, I've looked into that and it's technically sophisticated, it's data protection friendly, so I'm happy with that.'" (Hornung, Interview)

The pseudonymity function became embedded into the cryptographic architecture of the e-ID system. The power of the data protection community of practice is evident here. A single individual was largely responsible for embedding the normative bias towards data minimisation, context separation and a bias against profiling into a technical architecture that will be in place for decades to come. Holding some form of identity document is mandatory for Germans 16 and over, and all citizens will possess an e-ID (or a passport) by 2020 due to the eventual invalidation of all paper IDs. The concretisation of core data protection principles in hardware and cryptography shows the technocratic character of e-ID policy-making, as well as an exercise of power by data protection practitioners. It is an example of Meyer and Rowan's (1977) assertion that powerful actors can build their goals directly into society as institutional rules; in this case, their goals are built materially. Still, that power

is limited to the actors' sphere of influence: the e-ID. International business' lack of interest in becoming certified to access the personal data on the e-ID means that this power is limited to e-government and the low number of certified private German companies. A recent example, however, of the extent of the power of German DPAs over non-German businesses can be found in a 2012 declaration by the ULD that Facebook violates German law requiring the option for pseudonymous use of internet services (ULD, 2012). The subsequent resulting injunction was defeated in a state court; the case was appealed and awaits action at the time of this writing (Jaeger, 2013).

The US shows similar signs of the power of the data protection community in the development of its identity management policy. A special subcommittee of the Federal CIO Council was formed to address privacy considerations of citizen-focused identity management. Respondents involved in discussions with FICAM cite slowdowns in the policy development to allow for internal privacy debates (G001, Interview; G003, Interview; P006, Interview). Prior to the enactment of FICAM's citizen-specific policies, members of the CIO Council privacy subcommittee reviewed the policies and required changes before going forward. This was a 'veto point,' in Immergut's (1990) language; a contestation between the logic of data protection and the logic of e-government, which would otherwise move the policies forward in service of efficiency.

Like Germany, a number of formal policy instruments in the US exert coercive or normative influence over information policy formation. The US can be seen as having weaker, less coherent data protection institutions in comparison with Germany due to its lack of omnibus data protection legislation and data protection authorities. In recent years, the Federal Trade Commission (FTC), an agency charged with protecting consumers from unfair, deceptive or anti-competitive practices, has published a number of reports to encourage privacy

in the world of accelerating technology. The 2012 FTC report, "Protecting Consumer Privacy in an Era of Rapid Change," specifically evaluates issues regarding the linkability of personal and non-personal data (Federal Trade Commission, 2012, pp. iv, 18-22). In 2008, the Department of Homeland Security (DHS), a large agency encompassing border security, immigration policy implementation, anti-terrorism activities, cybersecurity and emergency response management, published a guide to implementing privacy across its various departments in service of transparency and to serve as an example to other US agencies (U.S. Department of Homeland Security, 2008). The guide has the Fair Information Practice Principles as its core privacy rationale. Members of the DHS and FTC privacy staffs were part of the CIO Council subcommittee on privacy in identity management, and have been part of the larger community of practitioners affecting the norms and rules of data protection of citizen digital identities. In the US as in Germany, discussions about privacy in identity management have not risen to the legislature – they remain at the level of administrators, bureaucrats and agency policy-makers. Requirements for unlinkable credentials for e-government and the strongly worded normative language in the National Strategy for Trusted Identities in Cyberspace exhibit the exercise of power of the data protection community. Specific calls for the limiting of 'panopticality' or of the loss of "anonymity, unlinkability and unobservability" (United States Postal Service, 2013a, p. 5) underscore the technocratic nature of identity management policy. That nature provided opportunity for data protection practitioners to re-apply their values. These practitioners recognised their opportunity, as one senior identity management official noted:

> "I think that they relished the opportunity that they were being brought into the FICAM picture and [were] able to work on policies that would be implemented." (G003, Interview)

The scale of the opportunity was huge. The Federal Cloud Credential Exchange has been designed for 135 million users (U.S. Postal Service,

2013b). Requirements for unlinkability within the FCCX are symbolic of the power of a select group of data protection and privacy practitioners. As with Germany, this power is circumscribed by the specific policy domain: citizen identity management for e-government. However, use of the FCCX by citizens may impart a normative or cultural-cognitive influence, making unlinkability appear over time to be more appropriate than its absence.

Identity management and e-ID policy is fertile ground for data protection and privacy practitioners to apply recent thinking and normative values. Credentialing and identity technologies are complicated, particularised and potentially obscure. This renders their policy domains technocratic, providing an opportunity for the exercise of power by data protection professionals who can understand the technology and use the surrounding policy development as an opportunity to re-apply core data protection principles – minimisation, proportionality, context separation and a bias against profiling. The power of this community can be seen in the embedding of unlinkability requirements in technical designs for citizen identity management systems. Policy development at administrative and bureaucratic levels shields the evolution of privacy from the vicissitudes of political change within the legislature. This contributes to a more consistent application of "moral resources" (Offe, 2006, p. 19) and "sectoral virtues" (Offe, 2006, p. 16). The technocratic opportunity to advance data protection goals via IDM and e-ID policy is one explanation for the similar appearance of unlinkability in two different countries with substantially different policy histories and cultures.

Institutional Change

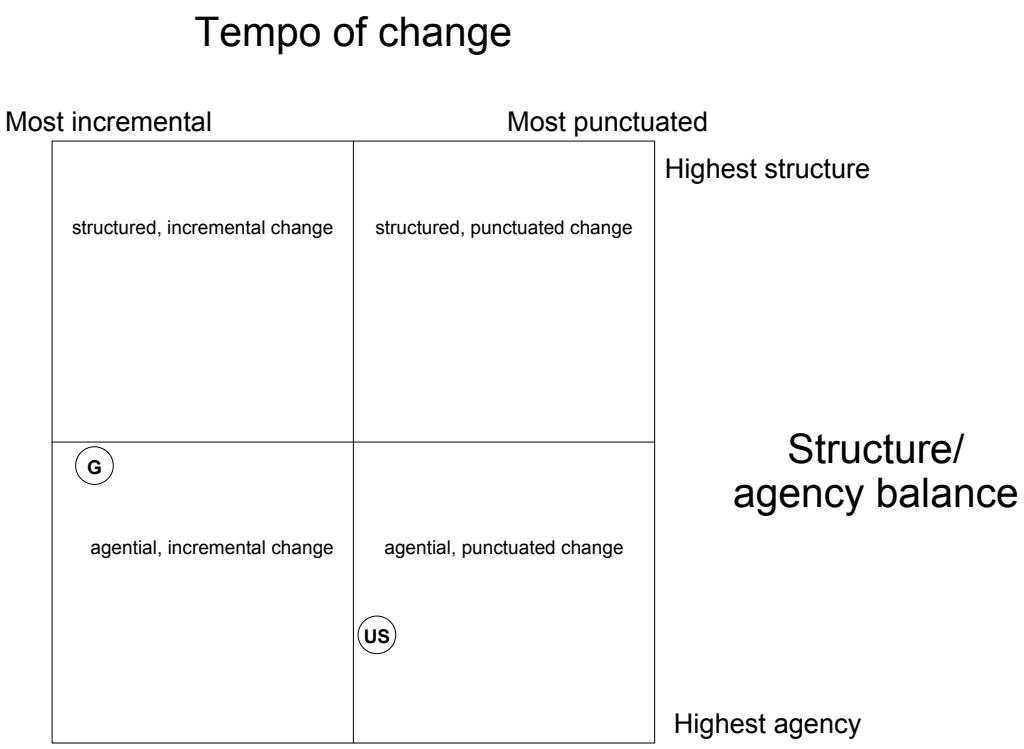
Lowndes and Roberts (2013, pp. 116-132) chart recent institutional theories of change against two analytic continua: the tempo of change, and the balance between structure and agency. This leads to four quadrants:

- structured, incremental change
- agential, incremental change
- structured, punctuated change
- agential, punctuated change

The use of unlinkability as a policy tool represents a change in the enactment of the institution of data protection. In both the US and German cases, agency plays a very strong role. Key groups of actors in both countries are largely responsible for the inclusion of unlinkability in the privacy and data protection regimes applied to citizen credentialing initiatives. However, the informal pressure to include German data protection authorities in the policy development process, the power of the 1983 Constitutional Court on subsequent data protection policy, and the power of the Ministry of Interior in setting the e-ID's agenda add structural elements to the explanation of the emergence of unlinkability. Such structural reasons are more weakly present in the US. The involvement of privacy lawyers from the CIO Council in the FICAM processes and the existence of the Fair Information Practice Principles were the core structural elements that influenced the inclusion of unlinkability.

In Germany, given the pseudonymity requirements of the Federal Data Protection Act and the Telemedia Act, the right to informational self-determination, and the requirement to separate the state into different informational contexts, German unlinkability is an incremental change. The US is less incremental due to its lack of formal instruments requiring context separation or pseudonymity. Using Lowndes and Roberts' (2013, pp. 116-132) framework, Germany and the US can be mapped as follows:

Figure 8.1 Location of Germany and US on map of institutional change explanations



Source: adapted from Lowndes and Roberts, 2013, p. 117

Germany, represented by "G," appears very close to the maximum position for incremental change, but at a nearly central balance between agential factors and structural factors. The US reflects more a punctuated change than an incremental one, with higher agential factors than Germany. The map helps to visualise the comparative political relationship between the two countries with regard to the emergence of unlinkability. It provides additional context to explaining the particular influences in each country that led to convergent information policies.

Conclusion

This chapter applied the theoretical approach the new institutionalism in order to explain the similarities and differences between US and German policy-making. New institutionalism illuminates the various influences that explain the isomorphic emergence of unlinkability policies in two separate countries. Scott's and Lowndes' synthesis of new institutionalism, detailed in Chapter 2, are potent frameworks by which to approach policy analysis. The empirical data illustrates Scott's (2003, p. 881) view that

> "… most full-fledged institutions are made up of diverse elements. There are few 'pure' cases."

Institutionalism illuminates the material dimension of the reproduction and extension of the institution of data protection. This chapter attempted to answer Pinch's (2008, p. 461) call to theoretically account for technology: "… social theorists need to attend better to materiality: the world of things and objects of which technical things form an important class." Consideration of the institutional forces at work in identity management policy helps to explain the parallel appearance of unlinkability in two countries, and in future work may be fruitfully applied to research on the privacy dimensions of other nations, including Canada, Austria and the UK. Data protection is an institution, enacted by human actors and material technology. Information policy both subsumes and is subject to data protection. Identity management systems and electronic identity cards are recent technological innovations that affect and are affected by data protection. Policy scholarship of IDM and e-IDs must attend to institutional factors to try to understand the history and future of the fields.

This chapter found that new institutionalism aids in understanding how two different countries with varied approaches to the protection of personal privacy both arrived at a policy of unlinkability. Institutional dynamics in each country contributed to a reapplication of core data protection principles. While

Germany has a more coherent data protection and privacy regime than the US, the base principles informing each country's regime were similar and could be reapplied and innovated within the field of identity management. Prior policy commitments, both formal and informal, helped shape current policies. The isomorphic quality of German and US unlinkability policies reflect the values of the data protection community of practice, technologists, consultants and bureaucrats. In each country both actors and political structure influenced policy, contributing to the emergence of unlinkability. In Germany, structure and agency were largely balanced factors: a history of pseudonymity policies and requirements for context separation of information processing by the state, combined with the direct action of Jan Möller and others. Unlinkability was an incremental change in German information policy given the continual application and reinterpretation of data protection principles over the course of 40 years. Actors played a more decisive role in US information policy, taking it upon themselves to reinterpret historic and modern data protection principles in the absence of new legislation or other formal pressures. There were weaker structural factors leading to unlinkability than in Germany. The main structural factors were the 1974 Privacy Act, the privacy oversight subcommittee of the CIO Council, and the non-binding Fair Information Practice Principles. The tempo of change in the US was therefore punctuated – a significant change in the privacy regime.

Electronic identity is a complicated technical domain, replete with protocols, cryptography, and complex concepts of the fragmentary nature of the digital self. This caused policy-making to be technocratic, yielding an opportunity for data protection practitioners to assert their values and augment their national privacy regimes. Their commitments to the principles of proportionality, context separation, minimal disclosure and a bias against profiling were concretized in the servers, software and chips of identity management infrastructure. The cryptographic functions of the German e-ID and the

technical requirements of the proposed Federal Cloud Credential Exchange extend the institution of data protection. They are the vanguard of privacy-enhancing technology as policy, innovating and reifying 40-year old principles. Given the heterogeneity of information policy tools, and the diffuse institutions, laws, actors and influences that comprise the field, new institutionalism shows itself to be a helpful lens to bring the historical, cultural, political and technical into focus. It emphasises context over structure and function, and theorises the continuous and discontinuous elements of the protection of personal data. Information policy research benefits from this approach, reassembling the fragments of particular policies into a more visible whole.

New institutionalism has great explanatory power, but there is a danger for it to become all-encompassing. That is, it remains difficult to separate cultural practices, behaviour and political phenomena from institutions. Marriage, handshakes, the formal and informal rules of legislatures, Christianity, and the market are all said to be institutions by various scholars (Friedland and Alford, 1991; Greenwood, et al., 2008; Shepsle, 1989). There is a danger in such breadth: if an institution means everything, then the concept becomes imprecise. The boundary between an institution and its environment is blurry. It is further difficult to separate the concepts of 'institution' from 'institutionalisation.' To wit, is national identification in Germany an institution, or are national identity cards institutionalised? Therefore, is the analytical object the ID card, or the institution – laws, norms, mores, expectations, narratives – that gives rise to the material object? The utility of new institutionalism is challenged by these fine distinctions.

Institutionalism is helpful in explaining political and sociological phenomena, but these do not fully comprise all the dimensions of information policy. For example, the issue of usability factors strongly in both Germany and the US.

Policy intentions can be thwarted by poor design. Institutionalism is ill-suited to identify such areas – usability and design do not emerge from an analysis of institutional factors, yet they are significant in the realisation of policy goals.

CHAPTER 9: CONCLUSION

This thesis examined how unlinkability is emerging as public policy. The research found that it appears in various ways in the identity management policies of Germany and the US. The two countries have been constructing policies and infrastructures to supply their citizens with digital credentials for use with e-government and commercial websites. 'Identity management policy,' a sub-field of information policy, is an appropriate heading to capture the digital credentialing activities of governments and the privacy architectures therein. In both Germany and the US, IDM policy is affiliated with e-government initiatives. In Germany, IDM policy is strongly related to national identification, an institutionalised practice which stretches back into the early 20th century. This is not the case for the US, and the American polity's strong rejection of national identification is a crucial factor in explaining the current state of US citizen credentialing efforts. Unlinkability is a technical feature and a privacy strategy situated within identity management initiatives, so the former's fate is influenced by the latter's successes.

The appearance of unlinkability in the two countries is isomorphic – similar policies at similar times in similar domains. Given the lack of direct policy influence between the US and Germany on these issues, this isomorphism can be partly explained by institutionalist analysis. Indeed, to understand the parallel emergence of unlinkability, the key differences in its implementation and in citizen credentialing generally requires an examination of the institutional effects within the IDM policy field. In this way, the new institutionalist approach is helpful in theorising the under-theorised field of information policy. Information policy research benefits from a theoretical approach that is value-critical, and that examines local contexts, norms and power relationships in addition to formal policy instruments.

Data protection is itself an institution, sustained by laws, culture, expectations, norms, formal instruments and informal relationships. As an institution, it is enacted by human actors, such as data protection practitioners, and material technologies, such as cryptography. The institution of data protection exerted a strong pressure to include privacy-preserving elements within the new field of identity management policy as it emerged in Germany and the US. Digital identity, from a citizen or consumer perspective, is a recent phenomenon. It evolved alongside the internet, born of the need to identify users on local computer systems and to ensure that only they can access their authorised resources. Identity federation across organisational contexts and boundaries has contributed to the internet becoming a more identifiable place; a digital identity 'layer' is forming, with more and more identity transactions occurring. This research began by examining how regulation and policy would and could affect this layer. National identity management policies implicated the institution of data protection because those identities are made of personal data. The influence of that institution is powerful and visible in German and US policies to supply their citizens with digital identities. Its application in the field of identity management contributed to the field becoming the vanguard of each country's privacy regime.

The first explanation of unlinkability's emergence is the influence of prior data protection instruments. The proportionality principle appears in 1970 in Hesse, and in nearly all subsequent formulations of the core set of North American and European data protection principles. Proportionality's progeny, the principle of data minimisation, is also present in these formulations, and the two principles are direct antecedents of the choice to include unlinkability in IDM policy. In Germany, a strong bias towards context separation contributes to unlinkability's appearance. A seminal 1983 Constitutional Court case laid the legal foundation for the e-ID's pseudonymity function and German data protection as a whole. There is evidence as well of a pervasive culture of

privacy plus the influence of a vocal group of data protection authorities contributing to the policy choices that yielded unlinkability. In historical context, the German policy of unlinkability is an incremental policy change.

The US shares a data protection policy antecedent with Germany in the form of the Fair Information Practice Principles, which contain principles similar to those found in the EU Data Protection Directive and the German Federal Data Protection Act. Though non-binding, the FIPPs strongly influenced US policy, contributing to the choice to include unlinkability in citizen credentialing systems. Rather than having a prior legal commitment to context separation as in Germany, the FIPPs contain a principle of use limitation. However, recent US policy documents identify 'respect for context' as a privacy goal, bringing US privacy thought, if not law, closer to the German model (Federal Trade Commission, 2012; White House, 2012). Whether the policy goal is fairness, to frustrate illegitimate profiling, or to support one's right to informational self-determination through linkage control, unlinkability is a tool in the toolbox of data protection policies available to the state in its pursuit of privacy. Data protection's history and its current application and reinvention by a community of practitioners are key reasons that unlinkability appears in US and German IDM policy.

Institutions are sustained, or not, by human action; and there is competition among different institutions. Policies, too, require human action to come into being: unlinkability needed champions. Federated identity, cryptography, identity and attribute claims are esoteric, technical subjects. In terms of national policy-making, none of these rose to a level of substantive discourse in the legislatures of the two case study countries. Instead, IDM policy-making occurred at 'lower' levels – among administrators, bureaucrats, government lawyers, standards bodies and various interested parties. This protected identity management from the vicissitudes of electoral politics. IDM policy is a case of

multi-stakeholder governance, including actors from government, the business community, privacy advocates, computer scientists, standards communities and the professions. The voices of the data protection community were not the only ones competing for space to be heard. The codification of unlinkability and other privacy-preserving features is here evidence of the power of that community and their location within institutional arrangements. The multi-stakeholder governance of IDM, the presence of data protection and privacy practitioners during policy development, and the highly technical nature of citizen credentials gave those practitioners an opportunity to re-apply core privacy principles in the burgeoning digital identity layer. This is another example of the utility of an institutional perspective: the policy field is pregnant with many interests, and power is in flux. The strength of the privacy commitments in US and German IDM policy is a demonstration of the power and opportunism of the data protection and privacy practitioners who contributed to its policy development.

The lack of commercial interest in either providing online credentials to the American public or in accessing the German e-ID is exemplary of the logic of the market, a competing institution. US reliance on private actors rendered it more susceptible to market influence, hindering its policy goals more than in the German case. The institutionalised nature of identity credentials in Germany allowed for an easier path to the creation of the e-ID, whereas the US had to build its citizen IDM policies from scratch. The German Ministry of Interior had control over the development and, importantly, the implementation of IDM policy. In the US, implementation was given over to private actors who, so far, have not delivered what the government wants. Largely, this is because the government is not paying them to do so. The tension between government needs and market logic is evident in the US case, and authoritative general citizen credentials are still absent.

IDM and e-ID privacy requirements represent some of the most forward-looking data protection policies in their respective countries. This is most true in the US, which lacks the institutional coherence of Germany for these issues. For Germany, unlinkability was an incremental policy change, building upon the Federal Data Protection Act's and the Telemedia Act's pseudonymity requirements, the Constitutional Court's mandate that the state not be considered a single data processor, and the well-entrenched policies of data minimisation. For the US, it was more of a leap, given a lack of laws requiring pseudonymity, an absence of context separation requirements, and weakly supported minimisation requirements. The comparative method is useful here, illustrating the 'distance' each country had to travel to arrive at similar policies.

In both countries, unlinkability requirements are a rare appearance of privacy-enhancing technology as general policy aimed at citizens. In Germany, the cryptography generators embedded in each e-ID card are a reification of data protection principles; a multi-decade commitment to context separation and pseudonymity writ in silicon and plastic. The principles are reproduced and enacted in the online interactions of German citizens using their e-IDs. In the US, the unlinkability requirements of the Federal Cloud Credential Exchange will be no small feat – the envisioned cryptographic architecture is highly complex. No off-the-shelf product will suffice; it will require innovative, concerted engineering to meet privacy requirements yet also make the system auditable and able to fix problems when they arise within the projected population of 135 million users. The US's privacy requirements for the FCCX are a step towards greater institutional coherence by anchoring minimisation and context separation privacy goals in technical enforcement mechanisms. 'Code is law' in this respect: if the FCCX blinds identity providers from relying parties and relying parties from each other by default, privacy happens invisibly and with less reliance on human beings; this in the absence of

legislation. This enforcement model brings it closer to Germany, whose IDM architecture is mainly anchored in technical enforcement.

IDM's role as privacy vanguard can be seen in the formative governance of the US National Strategy for Trusted Identities in Cyberspace. The privacy subcommittee of the NSTIC's steering group has defined a set of privacy risks based on Solove's (2006) "A Taxonomy of Privacy." For the envisioned users of NSTIC-approved credentials, the 'ecosystem' must take heed of privacy risks such as "distortion," "exclusion," "appropriation," "loss of liberty," and "stigmatization" (Privacy Coordination Committee, 2013). Though these risks are embedded in the avowedly privately-led governance of national identity management efforts, they are remarkable for their significant advancement from the Fair Information Practice Principles and US privacy law. Though it lacks any formal instruments mandating informational self-determination, the US has edged closer to it through its identity management policies. Notably, the "appropriation" harm above is defined as "Personal data is used in ways *that deny a person self-determination* or fair value exchange" (Privacy Coordination Committee, 2013, emph. added). A fruitful continuation of this research would be to directly compare the German informational self-determination right to the policies emerging from US identity management development. As the US moves closer to the German privacy model, it moves closer to the European model – the draft regulation to update European data protection and e-signature law draws directly upon German law with regard to pseudonymity (Albrecht, 2013, p. 76; see also Cannataci, 2008). Further, the right to informational self-determination could be used as a metric by which to measure privacy and data protection evolution in countries beyond the field of identity management. This would be especially salient in the US given its sectoral approach to data protection.

IDM technology is built upon standards. The organisations that develop and manage standards are institutional actors, and the resultant technologies are carriers of institutionalisation. Policy-makers must rely on technology to effect policy – if the standard cannot do something envisioned, it won't happen without alteration. Such alteration is subject to market conditions and the governance of the managing standards body. Conversely, standards that have privacy-features, such as unlinkable pseudonyms and selective disclosure of attributes, provide new tools for the policy toolbox. The values of standards communities are at work in IDM inasmuch as the values of policy administrators. Architecture is indeed politics (Kapor, 2006). The SAML community built the capability for a new (ephemeral) pseudonym to be sent each time a user returned to a website, making it so that the site could not recognize it was the same user. No commercial products implement this feature (N003, Interview), but it is there. An unused tool, a norm lying fallow. Values, the culture of privacy, laws, standards and technology are inseparable from each other.

A critical institution to consider in identity management research is the market. In the two cases, its influence is visible in different ways, and is ultimately responsible for hindering policy goals. Largely because of the spectre of national identification, the US elected to go to the market for its citizen credentials. The perceived political impossibility of deploying government credentials, even ones restricted only to e-government use, led the US to engage private for- and non-profit organisations to meet its needs for strongly authenticated citizens credentials. Ten years after the publication of a risk methodology to harmonise agency acceptance of external credentials, there are none for the general populace that can be used to reliably identify people. There is no business case to provide them – the US government, so far, has failed to create an identity market. Regarding universities and research institutions, there is not a compelling reason to adapt their systems. The key

problem is that government is not paying anyone to build or adapt credentialing systems to suit its needs. It is 'use cases vs. business cases' – government's idea of value is not mirrored in the private sector. It is as if the US government conceived of digital identities as a procurement process, but never bought the product, hoping instead that private enterprise would creatively find ways to profit.

Digital identity is a product. This is true in the US, where commercial companies make the credentials the government sought to take advantage of, and it is true in Germany, though there the government is the final manufacturer. The logic of the market – reducing costs to increase profits, building for multiple markets, the absence of social considerations in favour of returning shareholder value, shaping client interests to match product strategies – conflicts with the logics of government; ruling by mandate, the absence of a sales view, accountability and transparency, voter support. In Germany the market did not retard the release of credentials as in the US, but market logic still frustrates policy intentions. The e-ID was conceived as a way to help Germans interact in a trustworthy, privacy-preserving way online, both on e-government sites and commercial ones. To access the e-IDs, government must certify organisations. This certification costs money and requires staff attention. Only Germans and residents have an e-ID or its counterpart, the eAT. This means that the identity market is only the size of the German population and its residents. It is seemingly not enough, given the low number of non-government organisations who have gone through the certification process. The market is not convinced of the value of official, verified citizen personal data. In evaluating the effects of market actors becoming authoritative for citizen identities versus traditional official identities, the distinction between official data and commercially obtained or volunteered personal data is a factor. Research into the changing nature of citizen-government relations would benefit from further analysis of the impact of commercial identity

providers supplanting the state. Issues such as accountability, intervenability, privacy and transparency are vital to consider where private interests supply forms of citizen identification.

The product nature of e-IDs can been seen in the main reason Germans are not activating the online authentication feature: weak marketing. The first and final point of contact for citizens and residents to get their e-ID is a staff member of a municipal office – in essence, a 'salesperson.' The citizen or resident ('customer') needs product information to understand and value the product. Neither the salesperson nor the customer was armed with enough information to know or care about the online authentication functions of the e-ID, and so only 28% of the 18.5 million cards in circulation have it turned on (Bundesverwaltungsamt, 2013). A key recommendation of this research is that policy-makers attend more to the product nature of digital identity. Treating it as an extension of official identity, which was historically bound up in issues of movement and citizen-government interaction (Torpey, 1997), may blind policy-makers to digital identity's commoditised character. This is especially true where online citizen credentials are not compulsory, as with the US and Germany. When identity documents are compulsory, the question of their value to citizens is moot. When they are not but yet they still factor in policy goals, value to the citizen becomes essential. Here again the government use case collides with other needs – the need for citizens to care enough to avail themselves of online credentials, which is a function of the credential's perceived value. Government digital identities are entering a glutted market – Facebook, Google, mobile carriers and many others are already trying to be the 'identity gateway' for their customers. Governments may be ill-suited to compete and must reflect on whose interests the IDs are being deployed for. If it is their own interests – for example, to make public service delivery more efficient – they will have to work hard to convince their customers to buy their cards and ideas. Prior research shows that citizens will not readily take up

government digital credentials when there are established alternatives that sufficiently fulfil authentication needs (Kubicek and Noack, 2010). While digital identities can be viewed as a public service in and of themselves, governments must be careful not to treat them exclusively so. They ignore their commodity nature and their competitive profile at their peril.

Historically, citizen identification was the province of the state. Official identification cards, driver's licenses, statements of citizenship, birth certificates – the state held a monopoly of authenticity on people's identities. This is shifting. A major contrast between the German and US cases is the US reliance on market-based identities, which are also appearing in several other nations. Finland and Sweden are but two European countries with an 'ecosystem' of coexisting private and official digital identities. In May 2013, it was announced that Nigeria would release national identity cards underpinned by MasterCard technology (England and Wallis, 2013). Comparison of the US and Germany highlights the institutional effects when a country relies solely on the market for its identities versus 'in-house' production by government. It also shows the comparative method to be favourable to IDM and privacy research: the comparative effectiveness of US versus German IDM policy is analytically valuable in understanding each country and others. A valuable continuance of this research would be to analyse the German and US cases from the perspective of David Lyon's card cartel theory, which includes market pressure, the prerogatives of law enforcement and cybersecurity, and an isomorphic momentum from concentrated efforts by parties who stand to gain financially from digital identities. Such an examination would contribute to understanding the 'business of privacy' – how commercial influence advances or retards privacy evolution on national and international scales. This would require research on the policy influence of the card cartel, and locating alignments between government and commercial IDM and security narratives.

Returning to the product nature of digital identity, it remains to be seen if the value of privacy-preserving features in government identity products will outcompete commercial identity products with weaker privacy architectures. Conversely, commercial identity providers could potentially raise their privacy minimums to avoid looking illegitimate. US government stakeholders believe this to be possible (G007, Interview). Further investigation of the institution of data protection from the perspective of competitive market pressures will help to frame the emergence of PETs as policy. Much of the normative literature calling for PETs in policy-making does not address the competitive and financial aspects of business stakeholders in great depth. While governments can mandate privacy on the grounds of dignity and rights, commercial companies need incentive to build privacy into their products – someone needs to make money to make privacy happen.

Institutionalism illuminates the creation of new actors and their roles. In the US case data, the Trust Framework Providers are new actors in the domains of data protection and identity management. They are 'translation points,' interpreting and passing on privacy requirements from one set of stakeholders to another. Similar is the role of consultants. A steady stream of them in US policy development helped shape the course of national IDM policy. Their values emerged through the technocratic processes of developing citizen credentials and became invisibly codified in the protocols that knit together IDM systems. Their power contributed overall to that of the data protection community, and its application reflects the need for specialist knowledge in IDM policy-making.

This research found that usability is a key issue in unlinkability specifically, and privacy and citizen credentialing generally. Both German and American policy stakeholders take note of this. Here the market model for credential issuance potentially trumps government issuance – a panoply of private

organisations have a better chance and strong motivations to create more usable identity management products. Further, the companies engaged by the US government – Google, Yahoo!, PayPal and others – were already well-established internet companies with large teams of designers and usability experts. The German government, as sole supplier of both the e-ID and the AusweisApp, necessary to interact with the card online, was in a comparatively weak position to address usability. They also lacked any competitive pressure to create better software designs. The complexity of online credentials and the questionable value of privacy features to users necessitate sound usability design. The UK has learned this lesson, and has a vocal, dedicated team of usability and design experts constantly iterating interfaces and the user experience of the Identity Assurance Programme, a citizen identity management system for British e-government (Reichelt, 2013). A key recommendation of this research is that to compete in the identity market, governments will have to treat usability as critically as they do privacy, security and utility. Research into the successes and failures of the UK IDM usability design process would be extremely valuable to other countries still in the early design phase of national electronic identity systems.

There is much literature of the surveillance dimension of national identification, both traditional paper forms, and the electronic variety (Bennett and Lyon, 2008; Caplan and Torpey, 2001; Lyon, 2009). A key contribution of this research is empirical data on deliberate attempts by states to *not* know what its citizens are doing via their identity documents. Germany is a significant example, given its specific choices to build an e-ID architecture with no centralised servers capable of tracking the activities of its populace. If unlinkability is rare, unobservability is rarer still. Future research in this area could examine the risks to German policy intentions posed by the appearance of e-ID proxies who sit in between card holders and authorised service providers (relying parties). One IDM scholar intimately familiar with the

German architecture (Kubicek, Inteview) cited their potential threat to system security. More generally, there is much research to be done on the international convergence of policies that blind the state to its citizens' activities. Unobservability is less directly connected to historical data protection principles and is more closely aligned with anonymity. Van der Hof, Koops and Leenes (2009) examined anonymity in citizen-government relations. A fruitful line of research lies in the intersection of this work and unobservable IDM architectures. Empirical research into emergence of unobservability would add to scholarship on privacy by design and PETs, and would be of value to policy-makers in the design stage of citizen IDM systems.

In the US, the picture of such issues is different because of significant architectural differences. In Germany there is but one identity provider: the state. So, unobservability is possible because there is only one observer; one panoptic eye to shut. US IDM policy envisions a plurality of identity providers. The existing FICAM rules and architecture blind government agencies from one another at Level of Assurance 1 and 2 – linkability is possible at Levels 3 and 4 where meaningful names must be sent to relying parties. The state can attempt to deny itself some knowledge of citizens' e-government activity, but they can only go so far in terms of restricting the private organisations supplying the credentials. The FICAM rules acknowledge that identity providers will always know the mapping of real identities to pseudonyms, and so they have been enjoined from using their knowledge for activities beyond citizen credentialing and are forbidden from sharing what they learn with others. The forward-looking FCCX requirements take things further by attempting to blind identity providers as to the use of their credentials – a technical method in place of a social one. Again, the 'devil' is in the details, and the empirical work of this thesis explores the complex and iterative relationship between policy intent, business prerogatives, standards, and enforcement mechanisms. It illustrates national attempts at privacy by design

and shows the tension between a state's embrace of its people through identity documents and a bias against inappropriate profiling by creating context separation.

This research contributes to information policy scholarship by examining government intentions to foster 'trustworthy' transactions on the internet. The core definition of trust here is the ability to rely on the validity of a presented identity – that an identity can be trusted to be whom it purports. This is vital for e-government efforts, but US and German policies intend for this trust to grow beyond government needs. Here we see portents of digital identity as a public service, and government identity management policy as an attempt to be the rising tide that raises all ships. Future research in this area could try to align the discourse and policy tools of trust with those of privacy to see if one correlates with or influences the other. Trust is vaguer than privacy, and it remains to be seen how this popular word translates into policy priorities. Trustworthy digital credentials are a new policy priority, and this research contributes to information policy scholarship by analysing its appearance.

The US case shows a link between digital identity and risk management. If an identity is organisationally derived, crossing the boundaries of another organisation entails risk as one may not be able to fully account for the identity processes inside the other. Identities are local and trust is not transitive among disconnected organisations. For the US government to trust the identities supplied by external organisations, a risk management strategy had to be created – the Levels of Assurance. These external identities are confidence-rated as their authenticity is difficult to judge. This risk characteristic is less present in the German case because there is only one identity source, the state, and it carries the pedigree of being official. The perception of risk in accepting the government's credential is very low; it has a high degree of trust. Nonetheless, total elimination of fraud is impossible. Digital identity,

especially the federated kind, must be subject to a risk calculus. Europe is building a policy infrastructure to allow one country's e-ID to be used in another; for one member state to trust another member state's credential in order to provision public services. There is recognition that all credentials are not created equal. To allow, for example, Spain to trust Belgian e-IDs, a risk methodology very similar to the Levels of Assurance is being developed. The Secure Identity Across Borders Linked (STORK) project has promulgated its Quality Authentication Assurance (QAA) framework to address cross-border ID trust issues. Like its US counterpart, QAA has four levels of assurance in a credential (Hulsebosch, Lenzini and Eertink, 2009). A similar framework is at work in Britain's Identity Assurance Program (Cabinet Office, 2013). For governments, risk is an endemic quality to the use of digital identities for public services, and there is policy convergence between Europe and North America. These policy efforts are rising to the level of international standardisation. ISO/IEC 29115 (2013) mirrors the US and STORK four levels of assurance. These frameworks, however, do not address privacy – they address authenticity. Privacy runs along a different policy track. This study contributes to identity management research by analysing the intersection of risk management, standards and authentication.

This thesis contributes to information policy scholarship by providing empirical data on the link between digital identity and public services. Both case studies show that the needs of e-government are connected to citizen identity management initiatives. Concern of an informationally-intrusive state contributed to the privacy regimes in those initiatives. In turn, those regimes advanced the state of privacy in Germany and the US, yielding PETs as policy. As such, this thesis performs "analysis ... *of* policy-making" Turner (1997, p. 19), fulfilling a summative rather than formative role, though the recommendations in this Conclusion make some attempt at helping to shape future policy.

A core contribution of this research is the definition of identity management policy: *Identity management policy is the set of laws and policies enacted by governments and supranational bodies concerning the facilitation, procurement, use, liability, legal nature, interoperability, technologies, risk methodologies, lifecycle and privacy of digital identities for its citizens and employees. This includes physical and logical authentication, e-signature, and electronic identification technologies for access to physical and electronic resources.* Future IDM research can test this definition for accuracy and utility. The comparative method was instrumental in arriving at this definition. If only German policy were examined, for example, the risk management dimension of citizen credentials would not have become evident. This definition contributes to information policy scholarship by circumscribing a sub-field of policy inquiry, adding context to the concept of IDM.

The research contributes to institutional theory by applying it in a novel domain, identity management. In doing so, the study answers calls within information policy literature to apply social theory in order to better understand phenomena. Institutionalist theory offers a variety of perspectives by which to examine values and norms, and interrelationships among actors, organisations and technology. Institutionalism is used in a diverse set of fields, enabling it to be a powerful approach in the interdisciplinary field of identity management. It enables political and sociological analysis, and helps to conceptualise "the digital economy as an emergent, evolving, embedded, fragmented and provisional social production that is shaped as much by cultural and structural forces as by technical and economic ones" (Orlikowski and Barley, 2001, p. 154). This study contributes to information policy scholarship in particular by examining the political processes of identity management, which are underrepresented in academic research.

In particular, institutionalism is useful in integrating the formal and informal influences of policy development explanations. It shows the roles values, norms and culture play in the institutionalisation of data protection and identity management. The architecture of the internet is a battleground for competing institutions as much as it is for competing code. The institutional perspective analyses the relationship between the values of actors and the hardware and software that accomplishes policy goals. It contextualises the material aspects of policy development, situating them within a social and historical context.

With regard to unlinkability, the institutionalist perspective unites cultural, legal, and social factors in an explanation of its emergence. It helps to separate structure and agency features of unlinkability policies. Lowndes and Roberts' (2013, p. 117) map of institutional change (see p. 301) contextualises policy change within data protection, enabling further comparison between different countries' tempo of change, the influence of structural features, and the influence of actors. Future research on the privacy architectures of national IDM initiatives could use this map as a framework to compare policy change and analyse the balance of structural factors and the role and power of actors in the evolution of privacy.

Institutionalism draws attention to human actors, emphasising both key stakeholders and the role of intermediaries in the shaping of policy development. It highlights the "sector-specific ethos" (Offe, 2006, p. 16) influencing political choices, and demonstrates how values travel through informal routes, such as lexicons and standards communities. Through its examination of coercive, normative and mimetic mechanisms, it partly explains isomorphism in information policy.

Institutionalism is, of course, imperfect, and is by no means a way to construct a complete explanation of policy development. A central criticism of institution

is its imprecision. If the state, Christianity, capitalism, marriage, a handshake, the rules governing a legislature, and data protection are all institutions, what is not? The boundaries between an institution and its environment are unclear. And, while an informal influence such as a relational network is a carrier of institutionalisation, the mechanisms of influence are imprecise. As a theory, it is blind to certain kind of phenomena. Within the empirical data, the important factor of usability is unaccounted for within institutionalism, yet a holistic analysis of identity management policy must include it. Still, despite these problems, institutionalism is valuable in integrating the formal with the informal in the search for explanations of policy development, innovation and change. It is a valuable way of theorising within the under-theorised field of information policy in an interdisciplinary way.

This methods and theoretical approach of this thesis forms a framework that can be applied to future research. The definition of identity management policy can circumscribe a research domain. Within it, the methods of comparative policy study can frame the selection of cases for a particular IDM topic. Those cases can be analysed thematically, and then compared using a synthetic institutionalist approach. This approach would draw out the actors and institutions influencing the policy under study, emphasising the coexistence of formal and informal factors, the tempo of change in relation to the balance of structure and agency, the roles of values, norms and culture, and the institutional effects of material technologies in explaining policy development. While this approach would only yield a partial explanation for the policy phenomena, the interdisciplinary framework would examine the formal and the informal, the explicit and the implicit, and the social and historical context of the issues, and so broaden the depth of scholarship on information policy-making.

APPENDIX A: LIST OF INTERVIEW SUBJECTS

US Case Interview Subjects

G001, senior government identity management policy-maker and administrator
G003, senior government identity management policy-maker and administrator
G004, senior government identity management policy-maker and administrator
G006, senior government privacy lawyer
G007, senior federal government identity management administrator
G008, senior federal agency identity management administrator
G009, senior federal government identity management administrator
G010, senior government privacy lawyer
N002, identity management expert
N003, identity management expert and standards developer
N004, identity management federation expert
N005, privacy advocate
N006, privacy advocate and identity management expert
P001, group: commercial identity management, standards and privacy experts
P005, commercial identity management technology and standards expert
P006, commercial identity management technology and standards expert
P007, commercial identity management technology and standards expert
Don Thibeau, Chairman, Open Identity Exchange
Drummond Reed, former Executive Director of the Open Identity Exchange and the Information Card Foundation
Scott David, expert in contract law for identity management and counsel for the Open Identity Exchange
Richard Wilsher, principle architect of the Kantara Initiative Identity Assurance Framework and former principle architect of tScheme
Bob Morgan, senior architect of InCommon Federation, identity management expert and senior standards developer

Dazza Greenwood, identity management legal expert and MIT lecturer

Andrew Nash, Head of Identity at Google and senior identity management standards developer

Paul Trevithick, founder of the Information Cards Foundation and senior identity management standards developer

German Case Interview Subjects

DE-G001, senior government information security expert

DE-G002, senior government administrator

DE-G003, group: commercial e-ID experts

DE-G005, senior e-ID and information security academic

Jens Fromm, Head of e-ID Research Group, Fraunhofer FOKUS

Prof. dr. Gerrit Hornung, Chair of Public Law, IT Law and Legal Informatics, Institute of IT-Security and Security Law, University of Passau

Prof. dr. Herbert Kubicek, Director of the Institute for Information Management Bremen and Professor of Applied Computer Science, University of Bremen

Jan Möller, Officer at Federal Ministry of Interior

Dr. Marian Margraf, information security scientist at Federal Ministry of Interior

ULD, Independent Centre for Privacy Protection, data protection authority for the German state of Schleswig-Holstein. Interview group comprised of: Marit Hansen, Harold Zwingelberg, Ninja Marnau and an anonymous subject

APPENDIX B: TOPIC GUIDE

Regulation

Language used for unlinkability

Genesis of regulation

- Legal/Policy mandate
- Relationship of eGov credentials and regulation to e-sig, e-passport, e-ID
- Extant regulations that crosscut the new regulation (e.g., disclosure reqs for AML, anti-fraud, terrorism, federal recording of eGov site use, carve outs for law enforcement)
- Key actors
- Previous regulations that led to the current one (predecessors; failed regs)
- Timeline of major events
- Opposing views
- How did technical feasibility estimations factor when the regulations were being authored? (US: The community of practioners is very divided on many elements; there are only 2 possible technologies that can do unlinkability, and at least one does not do everything desired, etc.)

Separate, related state/regional regs or laws?

Under what circumstances can users be linked / pseudonymity be broken?

Mechanisms of enforcement & audit

Justification for regulation

- Relationship of regulation to historical privacy and data protection regimes
    - US: FIPPs, what else?
    - Germany: forbidden unique identifiers, EC DPD, what else?
    - Are there international or professional influences on the regulations?
- Underpinning moral/ethical/political discourse
- What problem does the regulation address?

Relationship between unlinkability and desired linkability.

How unlinkability relates to concerns of unique identifiers

[US: relationship to REAL-ID]

Resistance to the regulation's implementation

Current status of the regulation

What do you think of the regulation? Good? Bad?

Is there feedback to the regulators?

How does the government "trust" that the system does what it's supposed to do?

The regulation's effect on non-eGov use

What is the cost of compliance?

What does success of the regulation look like (in 5 years, in 10)?

[add questions of inefficiency and rejection of data sharing btwn agencies]

Technical

What is the overall architecture of the eGov credentialing system?

How is unlinkability achieved?
- How is it measured?
- Are their contrary positions as to the security or privacy of the system?

Who are the key actors?
- In the supply chain
- In oversight
- Which department/entity "owns" the eGov credentialing?

How was the system tested/certified?

How is the system audited?

How does the system accommodate legal re-linking?

What is process that translated the policy into technical specs?
- How was the process managed?
- How were ambiguities handled?

- How does the government "trust" that the system does what it's supposed to do?

Is there a functional difference between use of the system for eGov versus non-government sites?

How are change requests handled?

Are there international or professional influences on the technology?

BIBLIOGRAPHY

ABC4Trust. (2012). Consortium. Retrieved from https://abc4trust.eu/index.php/home/consortium

Act on Identity Cards of 18 June 2009 (Federal Law Gazette I, p. 1346), amended by Article 4 of the Act of 22 December 2011 (Federal Law Gazette I, p. 2959).

A.L.A. (n.d.). The USA PATRIOT Act. Retrieved 15 Aug 2012, from http://www.ala.org/advocacy/advleg/federallegislation/theusapatriotact

Adams, A., Murata, K. and Orito, Y. (2010). The Development of Japanese Data Protection. *Policy & Internet, 2*(2), 95-126.

Adjei, J. (2013). Towards a trusted national identities framework. *info 15*(1), 48-60.

Agre, P. (2003). Information and Institutional Change: The Case of Digital Libraries. In A. Bishop, N. Van House & B. Buttenfield (Eds.), *Digital Library Use: Social Practice in Design and Evaluation* (pp. 219-240). Cambridge: MIT Press.

Aichholzer, G. and Strauβ, S. (2010). Electronic identity management in e-Government 2.0: Exploring a system innovation exemplified by Austria. *Information Polity, 15*(1), 139-152.

Albrecht, J. (2013). *Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data*. Retrieved from http://www.huntonprivacyblog.com/wp-content/uploads/2013/01/Albrecht-Report-LIBE.pdf

American Bar Association Identity Management Legal Task Force. (2011). Solving the Legal Challenges of Online Identity Management: Part 1, Identity Management Fundamentals and Terminology. Retrieved from http://meetings.abanet.org/webupload/commupload/CL320041/newsletterpubs/ABA-IdM-Report--Part-1--Draft-12-30-11.pdf

Anckar, C. (2008). On the Applicability of the Most Similar Systems Design and the Most Different Systems Design in Comparative Research. *International Journal of Social Research Methodology 11*(5), 389–401.

Baldwin, A., Mont, M. and Shiu, S. (2007). *On Identity Assurance in the Presence of Federated Identity Management Systems.* Bristol: HP Laboratories. Retrieved from http://www.hpl.hp.com/techreports/2007/HPL-2007-47R1.pdf

Bauer, M., Meints, M. and Hansen, M. (Eds.). (2005). D3.1: Structured Overview on Prototypes and Concepts of Identity Management Systems. Retrieved from http://www.jipdec.or.jp/archives/PKI-J/shiryou/e-auth_policy/fidis-d3.1.overview_IMS_E.pdf

BBC. (2013 May 31). Census reveals German population lower than thought. Retrieved from http://www.bbc.co.uk/news/world-europe-22727898

Bellamy, C. and Taylor, J. (1996). New information and communication technologies and institutional change: The case of the UK criminal justice system. *International Journal of Public Sector Management, 9*(4), 51-69.

Bellamy, C. and Taylor, J. (1998). *Governing in the Information Age*. Maidenhead: Open University Press.

Benbasat, I., Goldstein, D., and Mead, M. (2002). The Case Research Strategy in Studies of Information Systems. In M. D. Myers & D. E. Avison (Eds.), *Qualitative Research in Information Systems.* London: SAGE.

Bender, J., Kugler, D., Margraf, M. and Naumann, I. (2010). Privacy-friendly revocation
management without unique chip identifiers for the German national ID card. *Computer Fraud & Security 9*, 14-17.

Bennett, C. (1992). *Regulating Privacy: Data Protection and Public Policy in Europe and the United States.* Ithaca: Cornell University Press.

Bennett, C. and Lyon, D. (Eds.). (2008). *Playing the Identity Card*. London: Routledge.

Bennett, C. and Raab, C. (2003). *The Governance of Privacy: Policy instruments in global perspective*. Aldershot: Ashgate.

Bentham, Jeremy (1995). *The Panopticon Writings*. London: Verso.

Bhargav-Spantzel, A., Camenisch, J., Gross, T., and Sommer, D. (2007). User centricity: A taxonomy and open issues. *Journal of Computer Security, 15*(5), 493-527.

Bjorck, F. (2004). Institutional theory: A new perspective for research into IS/IT security in organisations. Paper presented at the 37th Hawaii International Conference on System Sciences, Big Island, HI.

Braman, S. (1989). Defining Information. *Telecommunications Policy, 13*(3), 233-242.

Braman, S. (2003). Introduction. In S. Braman (Ed.), *Communication Researchers and Policy-making* (pp. 1-9). Cambridge, Mass.: MIT Press.

Braman, S. (2003). The Long View. In S. Braman (Ed.), *Communication Researchers and Policy-making* (pp. 11-31). Cambridge, Mass.: MIT Press.

Braman, S. (2004). The Emergent Global Information Policy Regime. In S. Braman (Ed.), *The Emergent Global Information Policy Regime* (pp. 12-37). Basingstoke: Palgrave Macmillan.

Braman, S. (2004). Introduction. In S. Braman (Ed.), *The Emergent Global Information Policy Regime* (pp. 1-11). Basingstoke: Palgrave Macmillan.

Braman, S. (2006). *Change of State: Information, Policy, and Power*. Cambridge, Mass.: MIT Press.

Braun, V. and Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77-101.

Breitner, M. (2003). E-Government activities in Germany: Highlights and difficulties. Retrieved from http://www.iwi.uni-hannover.de/lv/seminar_ss03/Heese/website/E-Government.pdf

Browne, M. (1997a). The field of information policy: 1. Fundamental concepts. *Journal of Information Science, 23*(4), 261-275.

Browne, M. (1997b). The field of information policy: 2. Redefining the boundaries and methodologies. *Journal of Information Science, 23*(5), 339-351.

Bryman, A. (1988). *Quantity and Quality in Social Research.* London: Unwin Hyman.

Bryman, A. (2012). *Social Research Methods.* Oxford: Oxford University Press.

Buchwald, C. (1998). Public Policy Theory as a Framework for Studying Information Policy: The Case of Canada's Coalition for Public Information. Paper presented at the Canadian Association for Information Science.

Bundesverwaltungsamt. (2013). Der neue Personalausweis: Office for assignment of authorization certification. [PowerPoint slides]. Public presentation.

Burger, R. (1993). *Information policy: a framework for evaluation and policy research.* Norwood: Ablex Publishing Corp.

Burkert, H. (1981). Institutions of Data Protection – An Attempt at a Functional Explanation of European National Data Protection Laws. *Computer Law Journal 3*(1), 167-188.

Burkert, H. (2012). Balancing informational power by informational power or Rereading Montesquieu in the internet age. In E. Brousseau, M. Marzouki & C. Méadel (Eds.), *Governance, Regulation and Powers on the Internet* (pp. 93-111). New York: Cambridge University Press.

Burt, E. and Taylor, J. (2007). *The Freedom of Information [Scotland] Act 2002: New Modes of Information Management in Scottish Public Bodies?* Glasgow: Caledonian Business School. Retrieved from https://www.ip-rs.si/fileadmin/user_upload/Pdf/Publikacije_ostalih_pooblascencev/Irska__raziskava_o_FOI.pdf

Burr, W., Dodson, D., Newton, E., Perlner, R., Polk, W., Gupta, S. and Nabbus, E. (2011). *Electronic Authentication Guideline. NIST Special Publication 800-63-1*. Gaithersburg: National Institute of Standards and Technology.
Busch, A. (2010). The Regulation of Privacy (Working Paper No. 26). Jerusalem: The Hebrew University. Retrieved from http://regulation.huji.ac.il/papers/jp26.pdf

Cabinet Office. (2013). Good Practice Guide: Identity Proofing and Verification of an Individual. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204448/GPG_45_Identity_proofing_and_verification_of_an_individual_2.0_May-2013.pdf

Camenisch, J., Shelat, A., Sommer, D., Fischer-Hübner, S., Hansen, M., Krasemann, H., Lacoste, G., Leenes, R. and Tseng, J. (2005). Privacy and Identity Management for Everyone. In *DIM '05, Proceedings of the 2005 workshop on Digital identity management* (pp. 20-27). ACM: New York.

Camenisch, J. and Van Herreweghen, E. (2002). Design and implementation of the idemix anonymous credential system. *Proceedings of the 9th ACM Conference on Computer and Communications Security* (pp. 21-30). New York: ACM.

Cameron, K. (2005). The Laws of Identity. Retrieved from http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf

Cannataci, J. (2008). Lex Personalitatis & Technology-driven Law. *SCRIPTed 5*(1). Retrieved from http://www.law.ed.ac.uk/ahrc/script-ed/vol5-1/editorial.asp

Caplan, J. and Torpey, J. (Eds.). (2001). *Documenting Individual Identity*. Princeton: Princeton University Press.

Cavoukian, A. (2006). *7 Laws of Identity: The Case for Privacy-Embedded Laws of Identity.* Ontario: Office of the Information and Privacy Commissioner. Retrieved from http://www.ipc.on.ca/images/Resources/up-7laws_whitepaper.pdf

Chappell, D. (2006). Introducing Windows CardSpace. Retrieved from http://msdn.microsoft.com/en-us/library/aa480189.aspx

CIO Council (2008). Information Security and Identity Management Committee (ISIMC) Charter. Retrieved from http://www.docstoc.com/docs/37387178/DRAFT---Security-and-Identity-Management-Committee-(SIMC)-Charter

Clarke, R. (1993). Computer Matching and Digital Identity. Retrieved from http://www.rogerclarke.com/DV/CFP93.html

Clarke, R. (1994a). The Digital Persona and its Application to Data Surveillance. *The Information Society (10)*2, 77-92.

Clarke, R. (1994b). Human Identification in Information Systems: Management Challenges and Public Policy Issues. *Information Technology & People 7*(4), 6-37.

Clarke, R. (1999). Identified, Anonymous and Pseudonymous Transactions: The Spectrum of Choice. Retrieved from http://www.rogerclarke.com/DV/UIPP99.html

Clarke, R. (2010). A Sufficiently Rich Model of (Id)entity, Authentication and Authorisation. Retrieved from http://www.rogerclarke.com/ID/IdModel-1002.html

Davies, S. and Hosein, G. (2007). *Identity Policy: Risks and Rewards.* London: The London School of Economics.

DeSimone, C. (2010). Pitting Karlsruhe Against Luxembourg? German Data Protection and the Contested Implementation of the EU Data Retention Directive. *German Law Journal (11)*3, 291-318.

De Soete, M. (2013). ISO Security Standardization: An update on ISO/IEC JTC 1/SC 27 IT Security Techniques. Retrieved from http://docbox.etsi.org/workshop/2013/201301_securityworkshop/01_introduction/iso_iecjtc1_sc27_desoete.pdf

DiMaggio, P. and Powell, W. (1983). The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields. *American Sociological Review, 48*(2), 147-160.

DiMaggio, P. and Powell, W. (1991). Introduction. In W. Powell & P. DiMaggio (Eds.), *The New Institutionalism in Organizational Analysis* (pp. 1-38). Chicago: University of Chicago Press.

Doty, P. (1998). Why Study Information Policy? *Journal of Education for Library and Information Science, 39*(1), 58-64.

Doyle, C. (2003). Libraries and the USA PATRIOT Act: Congressional Research Service, The Library of Congress. Retrieved from http://www.fas.org/sgp/crs/intel/RS21441.pdf

Dropbox. (n.d). How secure is Dropbox? Retrieved from https://www.dropbox.com/help/27/en

Duff, A. (2004). The Past, Present, and Future of Information Policy: Towards a normative theory of the information society. *Information, Communication & Society, 7*(1), 69-87.

England A. and Wallis, A. (2013 May 9). Nigeria signs up MasterCard to make dual-purpose identity card. Retrieved from http://www.ft.com/cms/s/0/ec36e0dc-b8be-11e2-a6ae-00144feabdc0.html

Esterberg, K. (2002). *Qualitative Methods in Social Research*. Boston: McGraw-Hill.

Eurobarometer. (2011). *Attitudes on Data Protection and Electronic Identity in the European Union*. Special Eurobarometer 359. Retrieved from http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

European Council. (1995). EU Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data. Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

European Council. (1999). EU Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. Retrived from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:en:HTML

European Council. (2012). Proposal for a Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0238:FIN:EN:HTML

European Network and Information Security Agency. (2011). Managing multiple electronic identities. Retrieved from http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/mami/at_download/fullReport

Fawcett, J. and Downs, F. (1992). *The Relationship of Theory and Research*. Philadelphia: Davis.

Federal Data Protection Act as amended (2003). Retrieved from http://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html#p0059

Federal Office for Information Security. (n.d.). Der neue Personalausweis. Retrieved from https://www.bsi-fuer-buerger.de/BSIFB/DE/SicherheitImNetz/Personalausweis/Personalausweis_node.html

Federal Office for Information Security. (2011). Technical Guideline TR-03127: Architecture electronic Identity Card and electronic Resident Permit. Retrieved from https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03127/BSI-TR-03127_en_pdf.pdf?__blob=publicationFile

Federal Trade Commission. (2012). Protecting Consumer Privacy in an Era of Rapid Change. Retrieved from http://www.ftc.gov/os/2012/03/120326privacyreport.pdf

FIDIS. (n.d.). About FIDIS. Retrieved from http://www.fidis.net/about/

Florêncio, D. and Herley, C. (2007). A Large-Scale Study of Web Password Habits. In *Proceedings of the 16th international conference on the World Wide Web.* (pp. 657-666). ACM: New York.

Friedland, R. and Alford, R. (1991). Bringing Society Back In: Symbols, Practices, and Institutional Contradictions. In W. Powell & P. DiMaggio (Eds.), *The New Institutionalism in Organizational Analysis* (pp. 232-263). Chicago: University of Chicago Press.

Fumy, W. and Paeschke, M. (2011). *Handbook of eID Security*. Erlangen: Publicis.

FutureID. (n.d.). FutureID: Shaping the Future of Electronic Identity. Retrieved from http://www.futureid.eu/index.php

Gallagher, D. and Lefkovitz, N. (2012 July 27). GSA OGP Announces an Industry Day on Federal Federated Identity Solutions. [blog post] Retrieved from http://blog.idmanagement.gov/2012_07_01_archive.html

Galperin, H. (2004). Beyond Interests, Ideas, and Technology: An Institutional Approach to Communication and Information Policy. *The Information Society, 20*(3), 159-168.

Gandy, O. (1993). *The Panoptic Sort.* Boulder: Westview Press.

Gellman, B. (2012). Fair Information Practices: A Basic History. Retrieved from http://bobgellman.com/rg-docs/rg-FIPShistory.pdf

Geertz, C. (1973). Thick description: Towards an interpretive theory of culture. In C. Geertz, *The Interpretation of Cultures,* (pp. 3-30). New York: Basic Books.

Gigya. (2013). The Landscape of Social Login & Sharing: Consumers Want Choice. [blog post]. Retrieved from https://blog.gigya.com/the-landscape-of-social-login-sharing-consumers-want-choice/

Gov.uk. (n.d.). Identity Assurance. Retrieved from https://www.gov.uk/service-manual/identity-assurance

Government Paperwork Elimination Act of 1998, Pub.L. 105–277 Title XVII.

Graf, C., Hochleitner, C., Wolkerstorfer, P., Angulo, J., Fischer-Hübner, S. and Wästlund, E. (Eds.). (2011). Towards Usable Privacy Enhancing Technologies: Lessons Learned from the PrimeLife Project. Retrieved from

http://primelife.ercim.eu/images/stories/deliverables/d4.1.6-towards_usable_pets-public.pdf

Granovetter, M. (1985). Economic Action and Social Structure: The Problem of Embeddedness. *American Journal of Sociology, 91*(3), 481-510.

Greenwald G. and MacAskill, E. (2013 June 7). NSA Prism program taps in to user data of Apple, Google and others. *The Guardian*. Retrieved from http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Greenwood, R., Oliver, C., Sahlin, K. and Suddaby, R. (2008). Introduction. In R. Greenwood, C. Oliver, K. Sahlin & R. Suddaby (Eds.), *The SAGE Handbook of Organizational Institutionalism.* London: SAGE.

Grönlund, Å. (2010). Electronic identity management in Sweden: governance of a market approach. *Identity in the Information Society, 3*(1), 195-211.

Hall, P. and Taylor, R. (1996). Political Science and the Three New Institutionalisms. *Political Studies, 44*(5), 936-957.

Halperin, R. and Backhouse, J. (2008). A roadmap for research on identity in the information society. *Identity in the Information Society, 1*(1), 71-87.

Hammersley, M. (1992). *What's Wrong with Ethnography?* London: Routledge.

Hansen, M. (2008a). Linkage Control – Integrating the Essence of Privacy Protection into IMS, *Proceedings of eChallenges e-2008.* (pp. 585-1592). Stockholm, Sweden.

Hansen, M. (2008b). User-controlled identity management: the key to the future of privacy? *International Journal of Intellectual Property Management, 2*(4), 325-344.

Hansen, M. (2012). Top 10 Mistakes in System Design from a Privacy Perspective and Privacy Protection Goals. In J. Camenisch, B. Crispo, S. Fischer-Hübner, R. Leenes, & G. Russello. (Eds.), *Privacy and Identity 2011, IFIP AICT 375*, (pp. 14–31). Dordrecht: Springer.

Hansen, M., Schwartz, A., and Cooper, A. (2008). Privacy and Identity Management. *IEEE Security and Privacy, 6*(2), 38-45.

Hare J. and Woodhill J. (2013). FCCX Requires Technology Innovation to Implement Policy Requirements. Retrieved from http://www.resilient-networks.com/page55.html

Hay, C. and Wincott, D. (1998). Structure, Agency and Historical Institutionalism. *Political Studies, 46*(5), 951-957.

Heidenheimer, A., Heclo H. and Adams, C. (1990). *Comparative Public Policy: The Politics of Social Choice in America, Europe, and Japan*. New York: St. Martin's Press.

Hildebrandt, M., Koops, B-J. and de Vries, K. (2008). D7.14a: Where Idem-Identity meets Ipse-Identity. Conceptual Explorations. Retrieved from http://www.fidis.net/fileadmin/fidis/deliverables/fidis-WP7-del7.14a-idem_meets_ipse_conceptual_explorations.pdf

Hoepman, J-H. (2012, May 8). The new German eId card has security, privacy and usability limitations. [blog post]. Retrieved from http://blog.xot.nl/2012/05/08/the-new-german-eid-card-has-security-privacy-and-usability-limitations/

Horsch, M. and Stopczynski, M. (2011). The German eCard-Strategy. Retrieved from http://www.cdc.informatik.tu-darmstadt.de/reports/reports/the_german_ecard-strategy.pdf

Hornung, G. and Roßnagel, A. (2010). An ID card for the Internet – The new German ID card with "electronic proof of identity". *Computer Law & Security Review 26*(2), 151-157.

Hornung, G. and Schnabel, C. (2009). Data protection in Germany I: The population census decision and the right to informational self-determination. *Computer Law & Security Report 25*(1), 84-88.

Hulsebosch, B., Lenzini, G. and Eertink, H. (2009). D2.3 - Quality authenticator scheme. Retrieved from http://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=577

IDABC (2009). eID Interoperability for PEGS: Update of Country Profiles study: German country profile. Retrieved from http://ec.europa.eu/idabc/servlets/Docc800.pdf?id=32302

Identity, Credential & Access Management (2009a). Identity Scheme Adoption Process. Retrieved from http://www.idmanagement.gov/documents/identityschemeadoptionprocess.pdf

Identity, Credential & Access Management. (2009b). OpenID 2.0 Profile. Retrieved from

http://www.idmanagement.gov/sites/default/files/documents/ICAM_OpenID20Profile.pdf

Identity, Credential & Access Management (2009c). Roadmap and Implementation Guidance. Retrieved from http://api.ning.com/files/cAuKrbWdEQePuzQxVnLMKFzYCcfBk-XqKqmTtZGekTu**h5br7dbU7slH*nDfRiosKLNpb-6Qg14KrPV8Z0vGl-dVUM1sktC/FICAM_Roadmap_Implementation_Guidance.pdf

Identity, Credential & Access Management (2009d). Trust Framework Provider Adoption Process For Levels of Assurance 1, 2, and Non-PKI 3. Retrieved from http://www.idmanagement.gov/documents/trustframeworkprovideradoptionprocess.pdf

Identity, Credential & Access Management. (2011a). Security Assertion Markup Language (SAML) 2.0 Web Browser Single Sign-on (SSO) Profile. Retrieved from http://www.idmanagement.gov/sites/default/files/documents/SAML20_Web_SSO_Profile.pdf

Identity, Credential & Access Management. (2011b). Roadmap and Implementation Guidance Version 2.0. Retrieved from http://www.idmanagement.gov/sites/default/files/documents/FICAM_Roadmap_and_Implementation_Guidance_v2%200_20111202_0.pdf

IDManagement.gov (n.d. a). Approved Identity Providers. Retrieved from http://www.idmanagement.gov/pages.cfm/page/ICAM-TrustFramework-IDP on 13 Jan 2013

IDManagement.gov (n.d. b). Approved Trust Framework Providers. Retrieved from http://www.idmanagement.gov/pages.cfm/page/ICAM-TrustFramework-Provider

Immergut, E. (1990). Institutions, Veto Points, and Policy Results: A Comparative Analysis of Health Care. *Journal of Public Policy 10*(4), 391-416.

InCommon. (n.d. a), Current InCommon Participants. Retrieved from http://www.incommonfederation.org/participants/

InCommon. (n.d. b), Assurance FAQ. Retrieved from http://www.incommon.org/assurance/faq.html

Independent Centre for Privacy Protection and Studio Notarile Genghini. (2007). Identity Management Systems (IMS): Identification and Comparison

Study. Retrieved from https://www.datenschutzzentrum.de/idmanage/study/ICPP_SNG_IMS-Study.pdf

Internet World Stats. (2013). World Stats. Retrieved from http://www.internetworldstats.com/stats.htm

ISO/IEC 7810 (2003). Identification cards – Physical characteristics. Retrieved from http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=31432

ISO/IEC 15408-1. (2009). Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model. Retrieved from http://standards.iso.org/ittf/PubliclyAvailableStandards/c050341_ISO_IEC_15408-1_2009.zip

ISO/IEC 24760-1. (2011). Information technology -- Security techniques -- A framework for identity management -- Part 1: Terminology and concepts. Retrieved from http://standards.iso.org/ittf/PubliclyAvailableStandards/c057914_ISO_IEC_24760-1_2011.zip

ISO/IEC 29115. (2013). Information technology -- Security techniques -- Entity authentication assurance framework. Retrieved from http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45138

Jaeger, M. (2013 Apr 26). No more fake names: German court sides with Facebook over pseudonym lawsuit. ZDNet. Retrieved from http://www.zdnet.com/no-more-fake-names-german-court-sides-with-facebook-over-pseudonym-lawsuit-7000014539/

Jepperson, R. (1991). Institutions, Institutional Effects, and Institutionalism. In W. Powell & P. DiMaggio (Eds.), *The New Institutionalism in Organizational Analysis* (pp. 143-163). Chicago: University of Chicago Press.

John, A. (2012 Sept 30). Challenges in Operationalizing Privacy in Identity Federations. [blog post] Retrieved from http://info.idmanagement.gov/2012/09/challenges-in-operationalizing-privacy.html

Kantara Initiative (2010). Identity Assurance Framework: Federal Privacy Profile. Retrieved from

http://kantarainitiative.org/confluence/download/attachments/41025670/IAF-US+Federal+Profile+v1-d8_ICAM.pdf

Katzan, H. (2011a). Ontology of Trusted Identity in Cyberspace. *Journal of Service Science, 4*(1), 1-11.

Katzan, H. (2011b). Review of the Cyberspace Policy and Trusted Identity Documents. *Review of Business Information Systems 15*(2), 43-49.

Katzenbach, C. (2012). Technologies as Institutions. In N. Just & M. Puppis (Eds.), *Trends in Communications Policy Research* (pp. 117-138). Chicago: University of Chicago Press.

Kent, S. and Millet, L. (2003). *Who Goes There? Authentication Through the Lens of Privacy.* Washington, D.C.: The National Academies Press.

Kerr, I., Steeves, V. and Lucock, C. (Eds.). (2009), *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society.* Oxford: Oxford University Press.

Kim, S., Kim, H. and Lee, H. (2009). An institutional analysis of an e-government system for anti-corruption: The case of OPEN. *Government Information Quarterly 26*(1), 42–50.

Kling, R., Lee, Y., Teich A. and Frankel, M. (1999). Assessing Anonymous Communication on the Internet: Policy Deliberations. *The Information Society, 15*(1), 79-90.

Koelble, T. (1995). The New Institutionalism in Political Science and Sociology. *Comparative Politics, 27*(2), 231-243.

Koops, B-J. and Leenes, R. (2005). 'Code' and the Slow Erosion of Privacy. *Michigan Telecommunications and Technology Law Review, 12*(1), 115-188.

Kubicek, H. (2010). Introduction: conceptual framework and research design for a comparative analysis of national eID Management Systems in selected European countries. *Identity in the Information Society, 3*(1), 5-26.

Kubicek, H. and Noack, T. (2010). The path dependency of national electronic identities. *Identity in the Information Society, 3*(1), 111-154.

Kuner, C. (2008). EU Data Protection: Proportionality Principle. *Privacy & Security*
Law Report, 7(44), 1615-1619.

Landau, S., Le Van Gong, H. and Wilton, R. (2009). Achieving Privacy in a Federated Identity Management System. In R. Dingledine & P. Golle (Eds.), *Financial Cryptography and Data Security Lecture Notes in Computer Science Vol. 5628*, (pp. 51-70). Dordrecht: Springer.

Lee, D. (2012 October 5). Facebook surpasses one billion users as it tempts new markets. Retrieved from http://www.bbc.co.uk/news/technology-19816709

Leenes, R. (2008). User-centric identity management as an indispensible tool for privacy protection. *International Journal of Intellectual Property Management, 2*(4), 345-371.

Lessig, L. (2006). *Code 2.0*. New York: Basic Books.

Levi, M. (1990). A Logic of Institutional Change. In K. Cook & M. Levi (Eds.), *The Limits of Rationality*. Chicago: University of Chicago Press.

Lijphart, A. (1975). The Comparable-Cases Strategy in Comparative Research. *Comparative Political Studies 8*(2), 158-177.

Lips, M. (2000). Designing Electronic Government Around the World. Policy Developments in the USA, Singapore, and Australia. *The EDI Law Review 7*(4), 199–216.

Lips, M., Taylor, J. and Organ, J. (2009a). Managing Citizen Identity Information in E-Government Service Relationships in the UK, *Public Management Review, 11*(6), 833-856.

Lips, M., Taylor, J. and Organ, J. (2009b). Identity Management, Administrative Sorting and Citizenship in New Modes of Government. *Information, Communication & Society 12*(5), 715–734.

Lim, T. (2010). *Doing Comparative Politics: An Introduction to Approaches & Issues*. Boulder: Lynne Rienner Publishers.

Lowndes, V. (1996). Varieties of New Institutionalism: A Critical Appraisal. *Public Administration, 74*(2), 181-197.

Lowndes, V. (2010). The Institutional Approach. In D. Marsh & G. Stoker (Eds.), *Theory and Methods in Political Science* (pp. 60-79). New York: Palgrave Macmillan.

Lowndes, V. and Roberts, M. (2013). *Why Institutions Matter: The New Institutionalism in Political Science*. Basingstoke: Palgrave Macmillan.

LSE Systems and Information Group. (2010). The Identity Project. Retrieved from http://identityproject.lse.ac.uk/

Lusoli, W., Maghiros, I. and Bacigolupo, M. (2008). eID policy in a turbulent environment: is there a need for a new regulatory framework?. *Identity in the Information Society, 1*(1), 173-187.

Lyon, D. (2003), Surveillance as Social Sorting: Computer Codes and Mobile Bodies. In D. Lyon (Ed.), *Surveillance as Social Sorting* (pp. 13-30). London: Routledge.

Lyon, D. (2009). *Identifying Citizens: ID Cards as Surveillance*. Cambridge: Polity Press.

Lyon, D. and Haggerty, K. (2012). The Surveillance Legacies of 9/11: Recalling, Reflecting on, and Rethinking Surveillance in the Security Era. *Canadian Journal of Law and Society 27*(3), 291-300.

Maler, E. (2011 Feb 8). OpenID, successful failures and new federated identity options. [blog post]. *ComputerworldUK.* Retrieved from blogs.computerworlduk.com/security-and-risk/2011/02/openid-successful-failures-and-new-federated-identity-options/index.htm

Maler, E. and Reed, D. (2008). The Venn of Identity: Options and Issues in Federated Identity Management. *IEEE Security and Privacy, 6*(2), 16-23.

March, J. and Olsen, J. (1984). The New Institutionalism: Organizational Factors in Political Life. *American Political Science Review, 78*(3), 734-749.

March, J. and Olsen, J. (2004). The logic of appropriateness. (Arena Working Paper WP 04/09). University of Olso. Retrieved from http://www.sv.uio.no/arena/english/research/publications/arena-publications/workingpapers/working-papers2004/wp04_9.pdf

Mariën, I. and Van Audenhove, L. (2010). The Belgian e-ID and its complex path to implementation and innovational change. *Identity in the Information Society, 3*(1), 27-42.

McCallister, E., Grace, T. and Scarfone, K. (2010). *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*. NIST Special Publication 800-122. Gaithersburg: National Institute of Standards and Technologies.

McClure, C., Moen W. and Bertot, J. (1999). Descriptive Assessment of Information Policy Initiatives: The Government Information Locator Service (GILS) as an Example. *Journal of the American Society for Information Science. 50*(4), 314-330.

McClure, C. and Jaeger, P. (2008). Government information policy research: Importance, approaches, and realities. *Library and Information Science Research, 30*(4), 257-264.

McCool, D. (1995). *Public Policy Theories, Models, and Concepts: An Anthology*. Englewood Cliffs: Prentice Hall.

Meckstroth, T. (1975). "Most Different Systems" and "Most Similar Systems": A Study in the Logic of Comparative Inquiry. *Comparative Political Studies, 8*(2), 132-157.

Meijer, A. (2003). Trust This Document! ICTs, Authentic Records and Accountability. *Archival Science, 3*(3), 275-290.

Meyer, J.and Rowan, B. (1977). Institutionalized Organizations: Formal Structure as Myth and Ceremony. *American Journal of Sociology, 83*(2), 340-363.

Modinis IDM Study Team (2005). Common Terminological Framework for Interoperable Electronic Identity Management – Consultation Paper, Version 2.01. Retrieved from https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/pub/Main/GlossaryDoc/modinis.terminology.paper.v2.01.2005-11-23.pdf

Mueller, M., and Lentz, B. (2010). Revitalizing Communication and Information Policy Research. *The Information Society, 20*(3), 155-157.

Nabeth, T. (2009). Identity of Idenity. In K. Rannenberg, D. Royer & A. Deuker (Eds.). (2009). *The Future of Identity in the Information Society* (pp. 19-69). Dordrecht: Springer.

Nissenbaum, H. (2010). *Privacy in Context*. Stanford: Stanford University Press.

Nithyanand, R. (2009). *The Evolution of Cryptographic Protocols in Electronic Passports.* Cryptology ePrint Archive, Report 2009/200. Retrieved from http://eprint.iacr.org/2009/200

Noack, T. and Kubicek, H. (2010). The introduction of online authentication as part of the new electronic national identity card in Germany. *Identity in the Information Society, 3*(1), 87-110.

North, D. (1991). Institutions. *Journal of Economic Perspectives, 5*(1), 97-112.

OASIS. (2013). OASIS Security Services (SAML) TC. Retrieved from https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

OpenID Foundation. (n.d.). OpenID Connect Work Group. Retrieved from http://openid.net/wg/connect/

Offe, C. (2006). Political Institutions and Social Power: Conceptual Explorations. In I.
Shapiro, S. Skowronek & D. Galvin (Eds.), *Rethinking Political Institutions: The Art of the State* (pp. 9-29). New York: New York University Press.

Office of Management and Budget. (2002). Memorandum M-03-03, Improving Customer Service By Establishing a One-Stop Recreation Reservation System. Retrieved from http://georgewbush-whitehouse.archives.gov/omb/memoranda/m03-03.html

Office of Management and Budget. (2003). Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002. Retrieved from http://www.whitehouse.gov/omb/memoranda_m03-22

Office of Management and Budget. (2007). Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information. Retrieved from http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf

Open Identity Exchange. (2013). What is a trust framework? Retrieved from http://openidentityexchange.org/what-is-a-trust-framework

Organization for Economic Cooperation and Development. (1980). OECD Guidelines on the
Protection of Privacy and Transborder Flows of Personal Data. Retrieved from http://www.oecd.org/internet/interneteconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

Organization for Economic Cooperation and Development. (2007). *At a Crossroad: "Personhood" and Digital Identity in the Information Society.* STI Working Paper 2007/7. Retrieved from http://www.oecd.org/dataoecd/31/6/40204773.doc

Organization for Economic Cooperation and Development. (2009). *The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers.* http://www.oecd.org/internet/ieconomy/43195291.pdfRetrieved from

Orlikowski, W. and Barley, (2001). Technology and Institutions: What can research on information technology and research on organizations learn from each other? *IS Quarterly, 25*(2), 145-165.

Orna, E. (2008). Information policies: yesterday, today, tomorrow. *Journal of Information Science, 34*(4), 547-565.

Ostrom, E. (1992). *Crafting Institutions for Self-Governing Irrigation Systems*. San Francisco: ICS Press.

Overman, E. and Cahill, A. (1990). Information Policy: A Study of Values in the Policy Process. *Policy Studies Review, 9*(4), 803-818.

Paquin, C. (2013). U-Prove Technology Overview V1.1. Retrieved from https://research.microsoft.com/pubs/166980/U-Prove%20Technology%20Overview%20V1.1%20Revision%202.pdf

Peters, B. (1998). *Comparative Politics: Theory and Methods*. New York: New York University Press.

Pfitzmann, A. and Borcea-Pfitzmann, K. (2010). Lifelong Privacy: Privacy and Identity Management for Life. In M. Bezzi, P. Duquenoy, S. Fischer-Hübner, M. Hansen & G. Zhang (Eds.), *Privacy and Identity Management for Life* (pp. 1-17). Dordrecht: Springer.

Pfitzmann, A. and Hansen, M. (2010). Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology (v0.34). Retrieved from http://dud.inf.tu-dresden.de/Anon_Terminology.shtml

Pinch, T. (2008). Technology as institutions: living in a material world. *Theory and Sociology, 37*(5), 461-483.

Poller A., Waldmann, U., Vowé, S. and Türpe, S. (2012). Electronic Identity Cards for User Authentication – Promise and Practice. *IEEE Security & Privacy 10*(1), 46-54.

Pontusson, J. (1995). From Comparative Public Policy to Political Economy: Putting Political Institutions in Their Place and Taking Interests Seriously. *Comparative Political Studies, 28*(1), 117-147.

Powell, W. and DiMaggio, P. (1991). *The New Institutionalism in Organizational Analysis.* Chicago: University of Chicago Press.

Poullet, Y. (2009). Data protection legislation: What is at stake for our society and democracy? *Computer Law & Security Review 25*(3), 211-226.

PrimeLife. (n.d.). About PrimeLife. Retrieved from http://primelife.ercim.eu/

Prins, C. (2006). When personal data, behavior and virtual identities become a commodity: Would a property approach matter? *SCRIPT-ed*, *3*(4), 270-303.

Privacy Act of 1974, 5 U.S.C. § 552a (1974).

Privacy and Security Tiger Team, (2012 Aug 10). DEA E-Prescribing for Controlled Substances: Identity Proofing & Authentication Requirements. [PowerPoint slides]. Retrieved from http://www.healthit.gov/sites/default/files/tiger_team_provider_authentication_08202012_final.pptx

Privacy Coordination Committee. (2013). Privacy Evaluation Methodology Workbook. Retrieved from http://www.idecosystem.org/filedepot_download/232/403

Programming4Us. (2010). Retrieved from http://mscerts.programming4.us/programming/identity%20and%20access%20management%20%20%20iam%20architecture%20and%20practice.aspx

Rahaman, A. and Sasse, A. (2010). A framework for the lived experience of identity. *Identity in the Information Society, 3*(3), 605-648.

Rannenberg, K., Royer D., and Deuker, A. (Eds.). (2009). *The Future of Identity in the Information Society.* Dordrecht: Springer.

Rannenberg, K., Sténuit, C., Yamada, A. and Weiss, S. (2007). Working Group 5: Identity Management and Privacy Technologies within ISO/IEC JTC 1/SC 27 – IT Security Techniques. Retrieved from http://www.itu.int/dms_pub/itu-t/oth/06/0D/T060D0000010011PDFE.pdf

Reding, V. (2013). EU Data Protection rules: Better for business, better for citizens. [speech]. Retrieved from http://europa.eu/rapid/press-release_SPEECH-13-269_en.htm

Reichelt, L. (2013 Aug 30). How we do user research in agile teams. [blog post]. Retrieved from http://digital.cabinetoffice.gov.uk/2013/08/30/how-we-do-user-research-in-agile-teams/

Reidenberg, J. (1997). Lex Informatica: The Formulation of Information Policy Rules Through Technology. *Texas Law Review 76*(3), 553-584.

Reiman, J. (1995). Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future. *Santa Clara Computer & High Technology Law Journal 11*(1), 27-44

Rein, M. (1976). *Social Science and Public Policy.* New York: Penguin.

Righettini, M. (2011). Institutionalization, Leadership, and Regulative Policy Style: A France/Italy Comparison of Data Protection Authorities. *Journal of Comparative Policy Analysis, 13*(2), 143-164.

Rissanen, T. (2010). Electronic identity in Finland: ID cards vs. bank IDs. *Identity in the Information Society, 3*(1), 175-194.

Robbin, A. (2000). Administrative Policy as Symbol System: Political Conflict and the Social Constuction of Identity. *Administration & Society, 32*(4), 398-431.

Rost, M. and Bock, K. (2011). Privacy by Design and the New Protection Goals. *DuD, January.* Retrived from http://maroki.org/pub/privacy/BockRost_PbD_DPG_en_v1f.pdf

Rouvroy, A. and Poullet, Y. (2009). The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy. In S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwangne, & S. Nouwt (Eds.), *Reinventing Data Protection?* (pp.45-76). Dordrecht: Springer.

Rowlands, I. (1996). Understanding information policy: concepts, frameworks and research tools. *Journal of Information Science, 22*(1), 13-25.

Rowlands, I. (Ed.). (1997). *Understanding Information Policy.* New Providence: Bowker-Saur.

Rowlands, I., Eisnenschitz, T. and Bawden, D. (2002). Frame analysis as a tool for understanding information policy. *Journal of Information Science, 28*(1), 31-38.

Schmidt, A. (2005). The German e-Card Strategy. [PowerPoint slides] Retrieved from http://fineid.fi/default.aspx?docid=3171&action=publish

Schmidt, V. (2005). Discursive Institutionalism: The Explanatory Power of Ideas and Discourse. *Annual Review of Political Science, 11*, 303-326.

Schmidt, V. (2009). Putting the Political Back into Political Economy by Bringing the State Back in yet Again. *World Politics, 61*(3), 516-546.

Schwartz, A. (2011). Identity Management and Privacy: a rare opportunity to get it right. *Communications of the ACM 54*(6), 22-24.

Scott, J. (1998). *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed.* New Haven: Yale University Press.

Scott, W. (1995). *Institutions and Organizations.* Thousand Oaks: SAGE.

Scott, W. (2003). Institutional carriers: reviewing modes of transporting ideas over time and space and considering their consequences. *Industrial and Corporate Change, 12*(4), 879-894.

Scott, W. (2008). *Institutions and organizations: Ideas and Interests*. Thousand Oaks: SAGE.

Scott, W. (2010). Reflections: The Past and Future of Research on Institutions and Institutional Change. *Journal of Change Management, 10*(1), 5-21.

SecureKey. (2013 Aug 21). SecureKey Technologies Wins Contract with U.S. Postal Service to Implement Federal Cloud Credential Exchange. [press release]. Retrieved from http://securekey.com/newsevents/securekey-technologies-wins-contract-with-u-s-postal-service-to-implement-federal-cloud-credential-exchange/

Shepsle, K. (1989). Studying Institutions: Some Lessons from the Rational Choice Approach. *Journal of Theoretical Politics, 1*(2), 131-147.

Shibboleth. (n.d). Shibboleth. Retrieved from http://shibboleth.net/

Sillince, J. (1994). Coherence of issues and coordination of instruments in European information policy. *Journal of Information Science, 20*(4), 219-236.

Silverman, D. (2001). *Interpreting Qualitative Data: Methods for Analysing Talk, Text and Interaction*. London: SAGE.

Simon, H. (1955). A Behavioral Model of Rational Choice. *Quarterly Journal of Economics, 69*(1), 99-118.

Sloan, R. and Warner, R. (2013). Beyond Notice and Choice: Privacy, Norms, and Consent. *Suffolk University Journal of High Technology Law, Forthcoming*. Retrieved from: http://ssrn.com/abstract=2239099

Small, M. (2004). Business and technical motivation for identity management. *Information Security Technical Report, 9(*1), 6-21.

Smart Card Alliance. (2012). *PIV-Interoperable Credential Case Studies.* Publication Number: IC-12001. Retrieved from http://www.smartcardalliance.org/resources/pdf/piv-i_case_studies_wp_022212.pdf

Solove, D. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review, 154*(3), 477-560.

Sprenger , P. (1999 Jan 26). Sun on Privacy: 'Get Over It'. *Wired.com*. Retrieved from http://www.wired.com/politics/law/news/1999/01/17538

Stake, R. E. (1995). *The Art of Case Study Research*. Thousand Oaks: SAGE.

Steiner, P. (1993 July 5). "On the Internet, nobody knows you're a dog". *The New Yorker, 69*(20), 61.

Steinmo, S., Thelen, K. and Longstreth, F. (1992). *Structuring Politics: Historical Institutionalism in Comparative Analysis.* Cambridge: Cambridge University Press.

Stevens, T., Elliot, J., Hoikkanen, A., Maghiros, I. and Lusoli, W. (2010). The State of the Electronic Identity Market: Technologies, Services and Policies: Institute for Prospective Technological Studies, JRC, European Commission.

Storf, K., Hansen, M. and Raguse, M. (2009). *Requirements and concepts for identity management throughout life*. PrimeLife H1.3.5. Retrieved from http://primelife.ercim.eu/images/stories/deliverables/h1.3.5-requirements_and_concepts_for_idm_throughout_life-public.pdf

Suchman, M. (2003). The contract as social artifact. *Law & Society Review, 37*(1), 91-142.

Tanenbaum, A. (1996). *Computer Networks.* Upper Saddle River: Prentice Hall.

Tavakoli, J. (2012 Nov 2). Facebook's Fake Numbers: 'One Billion Users' May Be Less Than 500 Million. [blog post] *Huffington post.* Retrieved from http://www.huffingtonpost.com/janet-tavakoli/facebooks-fake-numbers-on_b_2276515.html

Taylor, J., Lips, M, and Organ, J. (2008). Identification practices in government: citizen surveillance and the quest for public service improvement. *Identity in the Information Society, 1*(1), 135-154.

Telemedia Act. (2007). Translation by Centre for German Legal Information. Retrieved from http://www.cgerli.org/fileadmin/user_upload/interne_Dokumente/Legislation/Telemedia_Act__TMA_.pdf

Thelen, K. (1999). Historical Institutionalism in Comparative Politics. *Annual Review of Political Science*, 2, 369-404.

Thelen K. and Steinmo, S. (1992). Historical institutionalism in comparative politics. In S. Steinmo, K. Thelen & F. Longstreth (Eds.), *Structuring Politics: Historical Institutionalism in Comparative Analysis* (pp. 1-32). Cambridge: Cambridge University Press.

Torpey, J. (1997). Revolutions and freedom of movement: An analysis of passport controls in the French, Russian, and Chinese Revolutions. *Theory and Society, 26*(6), 837-868.

Torpey, J. (2000). *The Invention of the Passport*. Cambridge: Cambridge University Press.

Torpey, J. (2001). The Great War and the Birth of the Modern Passport System. In J. Caplan & J. Torpey. (Eds.). *Documenting Individual Identity.* Princeton: Princeton University Press.

Trauth, E. (1986). An integrative approach to information policy research. *Telecommunications Policy, 10*(1), 41-50.

Turning the tortoise into the hare: how the federal government can transition from old economy speed to become a model for electronic government, 107th Cong 2 (2002) (Testimony of Mark Forman). Retrieved from http://www.whitehouse.gov/sites/default/files/omb/legislative/testimony/mark_forman_032102.pdf

ULD. (2012 Dec 17). ULD issues orders against Facebook because of mandatory real names. [press release] Retrieved from

https://www.datenschutzzentrum.de/presse/20121217-facebook-real-names.htm

U.S. Census Bureau. (2013 June 12). U.S. and World Population Clock. Retrieved from https://www.census.gov/popclock/?intcmp=sldr1

U.S. Department of Health, Education and Welfare (1973). *Records, Computers and the Rights of Citizens*. Retrieved from https://epic.org/privacy/hew1973report/default.html

U.S. Department of Homeland Security. (2008). Privacy Policy Guidance Memorandum, Number 2008-01. Retrieved from http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf

U.S. National Science and Technology Council. (2008). *Identity Management Task Force Report*. Retrived from http://www.biometrics.gov/documents/idmreport_22sep08_final.pdf

U.S. Postal Service. (2013a Jan 10). Solicitation 1B-13-A-0003, Federal Cloud Credential Exchange (FCCX), Statement of Objectives. [Request for Proposals]. Retrieved from https://www.fbo.gov/?s=opportunity&mode=form&id=4012f1b6faa67c1dc791e8deb8dea7f8&tab=core&_cview=1

U.S. Postal Service. (2013b Jan 10). Solicitation 1B-13-A-0003, Federal Cloud Credential Exchange (FCCX), Appendix A, Requirements Matrix. [Request for Proposals]. Retrieved from https://www.fbo.gov/?s=opportunity&mode=form&id=4012f1b6faa67c1dc791e8deb8dea7f8&tab=core&_cview=1

Uteck, A. (2007). Ubiquitous Computing and Spatial Privacy. In I. Kerr, V. Steeves & C. Lucock, (Eds.), *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society* (pp. 83-102). Oxford University Press: Oxford.

van der Hof, Koops and Leenes (2009). Anonymity and the Law in the Netherlands. In I. Kerr, V. Steeves & C. Lucock, (Eds.), *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society* (pp. 503-521). Oxford: Oxford University Press.

van der Hof, S., Leenes, R. and Fennell, S. (2009). *Framing Citizen's Identities: The construction of personal identities in new modes of government in the Netherlands.* Nijmegen: Wolf Legal Publishers.

Valimo. (n.d.). Delivering a mobile eID for the whole nation – Case Finland. Retrieved from http://valimo.com/webfm_send/78

Waldo, J., Lin H. and Millet, L. (2007). *Engaging Privacy and Information Technology in a Digital Age.* Washington, D.C.: The National Academies Press.

Weerakkody, V., El-Haddadeh, R. and Al-Shafi, S. (2011). Exploring the complexities of e-government implementation and diffusion in a developing country: Some lessons from the State of Qatar. *Journal of Enterprise Information Management, 24*(2), 172-196.

Weingarten, F. (1989). Federal Information Policy Development: The Congressional Perspective. In C. McClure, P. Hernon & H. Releya (Eds.), *United States Information Policies: Views and Perspectives*. Norwood: Ablex Publishing Corp.

Weingarten, F. (1996). Technological Change and the Evolution of Information Policy. *American Libraries, 27(*11), 45-47.

Weir, M. (1992). Ideas and the politics of bounded innovation. In S. Steinmo, K. Thelen & F. Longstreth (Eds.), *Structuring Politics: Historical Institutionalism in Comparative Analysis* (pp. 188-216). New York: Cambridge University Press.

West, D. (2007). *State and Federal E-Government in the United States, 2007*. Retrieved from http://www.insidepolitics.org/egovt07us.pdf

White House (1993). Reengineering Through Information Technology. National Performance Review. Retrieved from http://govinfo.library.unt.edu/npr/library/reports/itexe.html

White House (2009). Cyberspace Policy Review. Retrieved from http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

White House (2011). National Strategy for Trusted Identities in Cyberspace. Retrieved from http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf

White House (2012). Consumer Data Privacy in a Networked World. Retrieved from www.whitehouse.gov/sites/default/files/privacy-final.pdf

Whitley, E. and Hosein, G. (2009). *Global Challenges for Identity Policies.* Basingstoke: Palgrave Macmillan.

Woodbeck, D. (2012 October 16). Virginia Tech First to Achieve Bronze, Silver. Retrieved from https://spaces.internet2.edu/display/InCAssurance/2012/10/16/Virginia+Tech+First+to+Achieve+Bronze%2C+Silver

Yin, R. (2009). *Case Study Research: Design and Methods.* London: SAGE.

Yusof, Z., Basri, M. and Nor, A. (2010). Classification of issues underlying the development of information policy. *Information Development, 26*(3), 204-213.

Zwingelberg, H. (2011). Necessary Processing of Personal Data: The Need-to-Know Principle and Processing Data from the New German Identity Card. In S. Fischer-Hübner, P. Duquenoy, M. Hansen, R. Leenes, & G. Zhang (Eds.), *Privacy and Identity Management for Life* (pp. 151-163). Dordrecht: Springer.

Zwingelberg, H. and Hansen, M. (2011). Privacy Protection Goals and Their Implications for eID Systems. In J. Camenisch, B. Crispo, S. Fischer-Hübner, R. Leenes, & G. Russello. (Eds.), *Privacy and Identity 2011, IFIP AICT 375*, (pp. 245-260). Dordrecht: Springer.