Future Internet **2013**, *5*, 34-45; doi:10.3390/fi5010034

OPEN ACCESS

future internet

ISSN 1999-5903

www.mdpi.com/journal/futureinternet

Essay

The Clean Privacy Ecosystem of the Future Internet

Lothar Fritsch

Norwegian Computing Center (Norsk Regnesentral), Gaustadalleen 23a/b, Kristen Nygaards hus, Oslo NO-0373, Norway; E-Mail: lothar.fritsch@nr.no; Tel.: +47-2285-2500

Received: 9 October 2012; in revised form: 7 December 2012 / Accepted: 6 January 2013 / Published: 14 January 2013

Abstract: This article speculates on the future of privacy and electronic identities on the Internet. Based on a short review of security models and the development of privacy-enhancing technology, privacy and electronic identities will be discussed as parts of a larger context—an ecosystem of personal information and electronic identities. The article argues for an ecosystem view of personal information and electronic identities, as both personal information and identity information are basic required input for many applications. Therefore, for both application owners and users, a functioning ecosystem of personal information and electronic identification is important. For the future of the Internet, high-quality information and controlled circulation of such information is therefore argued as decisive for the value of future Internet applications.

Keywords: information privacy; information security; privacy enhancing technology (PET); security perimeter; identity ecosystem; privacy

---

1. Introduction

Information privacy is discussed strongly in the face of social networks, search engine technologies, terabyte cloud storage services, and pervasive and mobile computing technologies. The future of Internet technologies might strongly depend on their ability to handle issues of power and freedom concerning authority over personal information, transparency, identification and interpretation based on others' data collection. In this article, I describe the origin of information privacy technologies. These technologies are not free of usability and economic considerations, which I discuss next. Finally, I speculate on the future of privacy regimes for Internet technologies and examine alternative perspectives beyond pure technological solutions for information privacy and identity protection on the future Internet.

2. Pre-Cryptographic Security Technologies

Privacy and data processing have had a tense relationship since data storage and computing power became available. Information privacy is an interdisciplinary domain connecting ethics, law, politics, technological development and business practice [1]. Within these domains, the technological aspects of data collection, data access, data distribution, and the respective policies and restrictions are in the focus of information privacy research. The journey to the future of Internet privacy begins in the deep middle ages of computing, where many of the classic access control mechanisms were developed to protect data bases and computing resources [2]. The computing resources of the time were centralized in computing facilities. Thus, the protection of the facility—the so-called security perimeter—was the main security activity. In addition, access to data and CPUs that were shared by many users had to be managed. Two major milestones where passed in this period: The classification of information into several levels of sensitivity, and the definition of user's roles with respective privileges to carry out operations on data.

2.1. Level Security Models as Early Data Protection Mechanisms

Multi-level security (MLS), invented in the 1970s, implements one out of two security goals, either confidentiality or integrity. Its name is derived from various levels of privileges needed by subjects to access data. MLS is a long-established and well-researched security concept that was developed for public and military administration and their confidentiality needs. Its basic assumption is that there are security levels from "public" to "top secret" that are assigned to documents or data sets. Access to documents is only allowed for users, programs or systems that have at least the same or higher security clearance than the object that is being accessed. Such classifications exist in many areas of government. There are several security models that specify MLS. The most important examples are Bell-LaPadula [3], Biba [4] and Lomac [5]. MLS is most concerned with managing access to data, and with protecting its integrity. It was clearly developed with large, centralized data processing in mind. Concerning privacy, MLS has a particular challenge where data has varying levels of sensitivity, which may even change over time.

2.2. The Appearance of Identity: Roles and Access Privileges per Person Appear

Multilateral security, in contrast to MLS, is not concerned with maintaining a leveled order as in the security models above. Multilateral security is concerned with the implementation of security between various actors (users, systems, processes) that might very well be on the same clearance level of MLS. Multilateral security models the relationships of systems to each other with respect to security issues. The goals of multilateral security can be complex and very different from each other. Thus, multilateral security is sometimes referred to as "policy-based security". Important models from multilateral security are Clark-Wilson [6], compartment/Lattice [7], Chinese Wall [8] and in the e-health arena, BMA [9]. Role-based models are important for information privacy handling, as they are not only concerned with a subject's "level" in data systems. They, in addition, introduce access policies of subjects to data. With these models, the explicit formulation of security policies that regulate the nature of personal data processing and the definition of the role of processors was

possible. Research in contemporary projects such as PRIME [10] and PrimeLife [11] enhanced role and policy models by defining complex privacy policy models, hardware-based trust management and obligations management [12].

3. Cryptography and the Erosion of the Security Perimeter

The major disruptive event on the security models of the 1970s was the dissolution of the security perimeter, where "personal" computers moved away from the centralized and protected infrastructures, while the larger systems became permanently connected to each other over communication lines, and ultimately, the Internet. This movement intensified the problems with access control, the movement of personal data to other computers, and worsened the ability to follow policies for data handling. The cryptographic techniques used to encrypt data bases and data links were based on symmetric cryptography, where all parties need to share a common key. Symmetric cryptography has, as a consequence, a high complexity in key handling and secure key distribution. It is, in addition, difficult to exclude parties who violate policies, as they can only be excluded with re-encryption of the data with a new key distributed to all other parties. The invention of public-key cryptography enabled much better handling of distributed multi-user and multi-computer scenarios, including the hierarchical certification of users and roles. In addition, researchers extended the uses of public key cryptography into a large number of higher cryptographic protocols that provide interesting properties such as multi-party secret sharing, anonymous authentication, blind attestation and secure group agreement.

3.1. Public Key Cryptography

The invention of public-key cryptography had two effects on data protection. First, the distribution and re-distribution of cryptographic keys was manageable in much better ways based on a public-key infrastructure (PKI). Second, based on a PKI, so-called certificates could be issued to users or organizations. Certificates can identify a person (and thereby constitute an electronic identity), or they can provide a role privilege. Here, a clear division in strategies for data protection turned up: the efforts divided into the re-establishment of perimeter security (by using PKI to extend the security perimeter through authenticated data links, authenticated identities and authenticated hardware and software) and into the efforts of establishing new paradigms (such as multi-party encryption, blind digital signatures, trusted platforms and data minimization). Many of the strategies to keep security guarantees up to defined levels included the re-erection of the security perimeter, wherein remote terminals or sessions had to perform additional security measures to be admitted to the still centralized main system resources. Encrypted data link lines, password security, code cards and one-time number generators are examples for additional security measures.

3.2. Higher Cryptographic Protocols for User Privacy

The next milestone in the dissolution of the safely centralized data processors was the wide uptake of computing in society, and especially in businesses and public administration. Both the processing of large amounts of personal data, and the wide and deep usage of computers by many humans in many places made the control of personal data increasingly difficult. This was a relevant phase where both

privacy and identity management challenges blossomed, and both research and practice thrived with the e-Commerce boom from the 1980s into the 1990s. Here, anonymizing MIXes for unobservable communication [13] were invented and extended from e-mail protocols to ISDN, mobile phones and IP [14], and researchers' imagination turned public-key algorithms into protocols with many peculiar properties in Identity Management (IdM), privacy preservation [15], secure electronic payments, and other areas. Some of the research results where reaching out into practice, for example the CAFÉ [16] and SEMPER [17] projects that developed or prototyped a number of technologies for electronic marketplaces including anonymous electronic cash, anonymous e-mail and Internet communication, revocable anonymity, e-cash with double spending control and blinding of certified information. The common assumption for most of these public-key cryptography based security protocols is that the private key part is safely, and exclusively, stored and used by the respective user or device only [17]. This assumption has made its way into regulatory frameworks such as the EU directive on electronic signatures [18].

3.3. Harnessing the Machine: Hardware Trust and Security Policies

On the other end, in the field of large databases and their applications, the insight that some personal data cannot be removed, but should get protected led to the extension of security models. By adding personal and role responsibility and auditability, models like Role-based Access Control (RBAC). RBAC has been published in 1992 [19]. The model has evolved since its first publication. It gained relevance in modern operating systems and other applications since. A current reference is the original inventors' book "Role Based Access Control" [20]. However, as the number of actors, databases and processors kept increasing, RBAC was facing addition complexity in defining and maintaining the sufficient policies over time. As a consequence of such evolving concepts of roles, large research projects such as PRIME and more recent ABC4Trust spent large parts of their efforts on syntactic and semantic definitions of roles and privileges in their respective policy expression languages and ontologies.

4. Privacy in the Age of Openness, Web Services, Mash-Ups and Profiles

The "final frontier" was the new millennium, where the "application perimeter" began to erode completely, dissolving classic pillars of information security such as proper relationships between computer owners, application owners, service owners and users into the "cloud", quickly eroding any isolated efforts in IdM through federation infrastructures. Web applications became composed web services that included other services as sub-services. Applications began to temporarily join with other applications for the purpose of application delivery. For information privacy, the consequence was the complete dissolution of the application border. It became nontransparent which services, or how many, were involved in a particular "web application". A key technology for such service composition was identity federation, a technology to partially join customer information within a certain service composition. The Liberty Alliance promoted an industrial standard which is now widely in use with large commercial actors on the web [21]. A second, much less complex protocol, OpenID [22], began to evolve as a single-sign-on (SSO) technology for web sites, promising to remove the burden of maintaining user accounts with many web applications, enabling cross-login from one application to

another. The mandatory personal profile on one social media platform now became the key to access other such platforms, thereby creating a profile-based SSO infrastructure with very limited information privacy properties. Research efforts such as the pseudonym-oriented social platform CLIQUE with its ability to use RBAC policies on all personal data [23] remained in the domain of research.

In addition, political pressure during the "war on terror" and successful industry lobby advocated identification technologies imposed on people (biometric passports, fingerprint scanning on airports, face recognition on surveillance cameras and records about movements and transactions), laying out the technological foundations of today's personalized, user-centric, and ubiquitous "Internet of Things" (IoT), a heterogeneous infrastructure of networks, computerized small devices and backend systems [24,25].

As an additional challenge, users sign into such infrastructures based on a new mobile "App-culture" based on always connected mobile personal devices, where everything is personalized and every interaction monitored, with actions enabling the construction of one or more technology-based personal identities in a connected world of billions of users. Locations are actually closely tied to identity and provide much additional information about a person's habits and preferences, and will, therefore, disclose personal attributes.

Anonymity and Privacy Enhancing Technology

While the new mobile and cloud-hosted technology paradigm was not yet defined, a number of research projects explored identity protection and privacy by means of higher cryptographic protocols. Many of the research efforts referred back to Chaum's MIX concept [13,26]. Their aim was the suppression of uncontrolled data release, along with strong confidentiality of communication relationships ("unobservability"). Many new terms and definitions have been collected and structured by Pfitzmann and Hansen [27]. A few alternative efforts to develop either a global, total infrastructure of identification, or a total, user-executed information control have been worked on by researchers. From the inventions made under the investigation of electronic cash [28], Brands credentials [29], the credential systems Idemix [30] and Microsoft's U-Prove [31] based on Brands were developed as protocols for anonymous or pseudonymous credentials [29,30], following suggestions for transaction pseudonymity made by David Chaum [32]. These credential systems are designed for unlinkable authentication and credential presentation. They were further researched with interdisciplinary efforts in building frameworks [33] for regulation, design, auditing and managing IT with guaranteed privacy properties and IdM systems with known risks. Large publicly funded research projects focused on user-centric privacy protection, on privacy-enhancing identity management, and on unobservable transactions on the Internet. Some of the results have made it into practice, such as the Tor project and AN.ON anonymization services [26], while a large part of the achievements is waiting for a debut with the user masses. In parallel, commercial developments have aimed at the re-introduction of a virtual security perimeter based on trusted hardware. In these, trustworthy software systems are expected to process data according to, and only according to, the processing policy that travels with the data [12]. Most of these developments targeted, however, the Internet paradigm based on personal computers. The largest part of the population these days is using services through mobile phone networks, an infrastructure that directly connects network access to identification, location and billing accounts.

Facing these growing infrastructures of identification, one expects resistance from its users. However, only a specialized segment of the user population insists on the use of PET. Investigations frequently show that strong anonymity technology that requires personal discipline and imposes an extra burden upon users is only accepted by special-interest groups [34–36]. General user populations frequently show little acceptance of security or privacy measures that impair user experience. Special-needs target groups frequently classify IdM technologies as one of the main hindrances for universal access to applications [37].

5. The Future of Internet Privacy

The future development of the Internet privacy infrastructure will face a number of challenges for technology development. In the area of usability, accessibility and e-inclusion, security technologies will need to develop according to varying user group's capabilities in different phases of their life [37]. Those organizations that deploy technology will become more interested in cost and economic issues—as well as the technology users. Finally, regulation might change the rules for running services and deploying technology on the future Internet. The following sections will discuss these issues.

5.1. Usability and e-Inclusion Issues

A usable and inclusive future Internet privacy infrastructure must take the goals, insights and concerns of various disciplines into account, especially those of Universal Design (UD) [38], security engineering and privacy and legal issues. By using UD, all potential users, with their different skills, knowledge, age, gender, (dis)abilities and literacy, can be included. A central issue in the field of UD of Information and Communication Technology (ICT) is the role of flexible multi-modal user interfaces that can meet different users' needs, abilities, situations, preferences and devices [39]. The paradigm in security engineering is often to design a single security method at a sufficient security level. However, the choice of this "one security method" will exclude many users from the use of many mainstream ICT supported products and services. The need for adaptability and flexibility in security and privacy technologies can be approached by personalization which may be based on user profiles holding information about the modalities and functionalities best suiting the particular user's individual needs and preferences, and by the use of assistive technology. Adaptability and usability will be challenges for the future Internet.

5.2. Economics, Balance of Effort, and Efficiency

User-centric identity management was developed to return the sovereignty over personal data use to the data subjects [33]. Many of the PET research efforts aimed at the re-establishment of user control, both concerning the release of identity information and the management of personal information. However, as important as these results are, there is a drawback. Each of their users has to invest extra efforts when "managing" their own privacy, or their many electronic identities in form of pseudonyms. Combined with real-world payment and delivery services, information privacy against web shops turns into difficult routine. Users who don't do so, gain more benefit from the applications they use by saving time, complexity and bad application quality. Service providers and system vendors don't gain

any benefits by making their own products more difficult to use by adding the latest privacy technologies, while their competition is still selling cheaper and provides a smoother user experience without them. Privacy economics might simply kill any good intentions, as argued by Roßnagel in [34]. Privacy economics refers to economic considerations and constraints concerning one's information privacy—both for system owners and users [40]. People often use a pragmatic approach to evaluate privacy risks against benefits when they use IT systems. In sharing, e.g., media objects, with friends, the immediate benefit is the feeling of community with friends or family. The management of access control, risk assessment concerning privacy, and fire-fighting of access errors however imposes cost—either in time used, loss of pleasure and usefulness, or real monetary cost. All explicit privacy handling, policy building and reconfiguring of access rules are costs imposed on users. It must be assumed that users will not invest more resources into managing privacy issues than they experience their perceived benefit of using a social network [41]. "Friends & family" privacy management is therefore more subject to interpersonal negotiation and re-negotiation than privacy regimes intended to control government or corporate data processing [42]. Rather explicit legal frameworks from these environments can hardly be translated into interpersonal relationships. It must be assumed that those who own power in social relationships will be in a better position to dominate the privacy regimes practically used. Not to mention the "Internet of Things", a term coined by Kevin Ashton in Procter & Gamble in 1999 [25,43]. The IoT is a networked environment where the user will be confronted with a complete cloud, or fog, of chips, devices, sensors and services from a multitude of stakeholders and peers. Increased complexity, uncertain policy consequences, and crude user interfaces for security and privacy policy handling are the main sources for usability issues.

5.3. Privacy and Electronic Identities as an Ecosystem

I imagine the future of Internet Privacy as part of an IT ecosystem with many interdependent systems and actors. One might view privacy issues in analogy to environmental pollution. Let's use the terms "personal information spill" for data breach, and for data transfer without consent of the person the data is about. There could be "Identity pollution", where too many e-IDs, accounts, passwords, e-mail addresses and banking tokens are imposed upon people, filling up useless databases with incomplete profiles of one-time customers, and user's minds with too many passwords, pseudonyms and fake accounts. The future of Internet Privacy will, in my opinion, depend on two factors: The quality (cleanness) of personal information and e-IDs in data bases, and the avoidance of personal information spill. The quality is more or less already asked for in data protection laws, as a combination of minimization, correctness, and transparency duties for data processors, but there are practically no checks and penalties for violation. However, many of the services on the horizon are dependent on good quality of data, e.g., about their users, to provide valuable services. Corporate value is calculated on the number of real user profiles, and the quality of such profiles, for example. Recent efforts of both Google and Facebook to join distinct pseudonyms used by the same users are illustrative—both in the ferocity they are carried out with, and in its side effects on stock value. To avoid constant quality assurance in future community-based or crowd-sourced applications, the win-win-situation might well be in a "clean" ecosystem of personal information aligned with both the user interest and the application purpose. As a side effect, parties that spill the ecosystem by providing

unreliable, poor-quality data, or by endangering community trust and application reputation, might be put at risk for sanctions by the other parties in self-regulatory approaches.

However, the measures to implement quality, and to avoid data spill poisoning the privacy ecosystem might be of a regulatory nature, and not based on pure technological solutions. Car catalyzers came after a law was introduced, and the same holds for many other measures in the area of pollution. The future of privacy might depend on bold regulatory frameworks that will increase quality and cleanness of the future Internet privacy ecosystem. Measures imaginable are not higher penalties for violation (though that is imaginable), but there could be an "environmental" tax on the number of person-related records, the number of customer profiles, the amount of collected personal data, or the amount of transactions ran against other parties involved. In addition, any information system processing personal data could be required to know the origin of the data, and should be able to make a statement about the quality and maturity of the personal data processed.

There might be automated metering stations (as deployed in polluted rivers) that constantly audit information systems to monitor what happens with personal data on them, with respect to the law and the policies and consent regulating personal data use. Such agents might be deployed by data protection authorities, by data subjects themselves, or by auditing third parties. In the e-health arena, due to the complexities of hospital IT systems and the large number of users floating from one department to another, such technical surveillance measures have begun to replace policy-based security measures on health records [44], as the only possibility to gain insight into data access in extremely heterogeneous IT systems.

One regulatory reaction is clearly foreseeable: There certainly will be fines and exclusions from government business for the worst violators, comparable to corruption blacklists. Harsher sanctions, such as blacklisting global actors that constantly violate local privacy laws on the filtering infrastructure made for fighting illegal content sites, might prove very efficient.

6. Conclusions

As the major upcoming challenge, I see the central question to be the power to control personal data use and e-ID use both in global and in "local" (to be interpreted in terms of cloud, or IoT6 local federations). Mireille Hildebrandt's threat to be read by others in wrong contexts based on data residing from another transaction is an essential issue here [45]. Transparency about data sources, and intervention capabilities for correction are already today part of privacy legislation (however, in most cases, a theoretical right against global providers).

Future monopolies of electronic identification, profiling and federation potentially exercise vast power over wide parts of the e-society, transcending local regulation, politics and societies. Answers to these challenges have, at least in many of the European research projects on privacy technology, been given only for the end users by supplying user-centric technologies, policy management tools, and user-controllable identity management systems.

The outlook on privacy and identity ecosystems presented above might not look overly brilliant for a smaller start-up business that seeks to get one million new users by the end of the year, and then sell out as fast as possible. However, a class action lawsuit under United States law, or an embargo against its service, carried out with the globally available IP filtering infrastructure installed for fighting child

pornography, racist propaganda or for censoring unwanted parties might put such a polluting player off the market in no time. I expect that a clean "identity and privacy ecosystem" will be in the best interest of all players, as it will offer long-term perspectives on user subscriptions, income, and compliance, while it ensures societal acceptance. I summarize the main elements of a future Internet privacy ecosystem as:

- Sustainable quality of personal information;
- Sustainable quality of electronic identities;
- Transparency and intervention capabilities for data subjects;
- Reliability of peers in delivering quality information;
- Data minimization and total cost of handling personal information in sync, e.g., with the information tax approach;
- Monitoring and sanctioning of information polluters.

Regulation oriented towards a privacy ecosystem might offer an arena for development of new technologies for its management:

- Metrics for assessment of data quality, anonymity metrics, metrics for the amount and density of personal data collection, metrics for security usability;
- Technologies for automated audit of data processors and data collections;
- Trust technologies that enable data processing by policy, such as suggested by Hewlett Packard [12];
- Technologies for information hiding or control while participating in applications, such as e.g. homomorphic cryptography or anonymous credentials;
- Technologies for the identification of ecosystem members, blacklisted entities, and compliant entities of the information ecosystem.

Due to the global nature of Internet services, user mobility over legislative borders, and application mobility in the Cloud, the basic definition of a framework for a privacy and identity ecosystem is, however, a demanding international process that can only effectively be carried out through international bodies governing legal cooperation and trade relationships. The governance framework for the future Internet should, therefore, not only be designed by technicians, but should be the subject of an intentional, political process setting the rules of societal control over a coming technology with vast potential for profiling, surveillance, domination and transparency of the private life, and at risk of judgment for incomplete, wrongful, outdated or fabricated data.

References

1. Fritsch, L. Privacy-respecting location-based service infrastructures: A socio-technical approach to requirements engineering. *J. Theor. Appl. E-Commer. Res.* **2007**, *2*, 1–17.
2. Martin, J. *Security, Accuracy, and Privacy in Computer Systems*; Prentice-Hall: Englewood Cliffs, NJ, USA, 1973.
3. Bell, D.E.; LaPadula, L.J. *Secure Computer Systems: Mathematical Foundations*; MITRE Corporation: Bedford, MA, USA, 1973.

4. Biba, K.J. *Integrity Considerations for Secure Computer Systems*; MITRE Corporation: Bedford, MA, USA, 1977.
5. Fraser, T. LOMAC: Low water-mark integrity protection for COTS environments. In *Proceedings of IEEE Symposium on Security and Privacy*, Berkeley, CA, USA, 14–17 May 2000; IEEE Computer Society: Berkeley, Washington, DC, USA, 2000; pp. 230–245.
6. Clark, D.; Wilson, D. A comparison of commercial and military computer security policies. In *Proceedings of IEEE Symposium on Security and Privacy*, Oakland, CA, USA, 27–29 April 1987.
7. Sandhu, R.S. Lattice-based access control models. *Computer* **1993**, *26*, 9–19.
8. Brewer, D.F.C.; Nash, M.J. The Chinese wall security policy. In *Proceedings of Symposium on Security and Privacy*, Oakland, CA, USA, 1–3 May 1989; IEEE Computer Society: Washington, DC, USA, 1989; pp. 206–214.
9. Anderson, R. A security policy model for clinical information systems. In *Proceedings of 15th Symposium on Security and Privacy*, Oakland, CA, USA, 6–8 May 1996; IEEE Computer Society: Washington, DC, USA, 1996; pp. 30–43.
10. PRIME Privacy and Identity Management for Europe. Available online: http://www.prime-project.eu (accessed on 6 January 2013).
11. PrimeLife—Privacy and Identity Management in Europe for Life. Available online: http://www.primelife.eu/ (accessed on 6 January 2013).
12. Casassa Mont, M.; Pearson, S.; Bramhall, P. Towards accountable management of identity and privacy: Sticky policies and enforceable tracing services. In *Proceedings of 14th International Workshop on Database and Expert Systems Applications*, Prague, Czech Republic, 1–5 September 2003.
13. Chaum, D. Untraceable electronic mail, return addresses, and digital pseudonyms. *Commun. ACM* **1981**, *4*, 84–88.
14. Federrath, H.; Jerichow, A.; Kesdogan, D.; Pfitzmann, A. Security in public mobile communication networks. In *Proceedings of IFIP TC 6 International Workshop on Personal Wireless Communications*, Prague, Czech Republic, 24–25 April 1995; pp 105–116.
15. Fischer-Hübner, S. IT-Security and Privacy: Design and Use of Privacy-Enhancing Security Mechanisms; Springer: Berlin, Germany, 2001.
16. Boly, J.-P.; Bosselaers, A.; Cramer, R.; Michelsen, R.; Mjølsnes, S.; Muller, F.; Pedersen, T.; Pfitzmann, B.; Rooij, P.D.; Schoenmakers, B.; Schunter, M.; Vallée, L.; Waidner, M. The ESPRIT project CAFE—High security digital payment systems. *Comput. Secur.* **1994**, *875*, 217–230.
17. Lacoste, G.; Pfitzmann, B.; Steiner, M.; Waidner, M. *SEMPER—Secure Electronic Marketplace for Europe*; Springer: Berlin, Germany, 2000.
18. *Community Framework for Electronic Signatures*; Commission of the European Union: Brussels, Belgium, 1999.
19. Ferraiolo, D.F.; Kuhn, D.R. Role-Based access controls. In *Proceedings of 15th National Computer Security Conference*, Baltimore, MD, USA, 13–16 October 1992; pp. 554–563.
20. Ferraiolo, D.; Kuhn, D.R.; Chandramouli, R. *Role-Based Access Control*; Artech House: Boston, MA, USA, 2003.
21. Cutler, R. *Liberty Identity Assurance Framework*; Version 1.1; Liberty Alliance Project: Piscataway, NJ, USA, 2008.

22. Recordon, D.; Reed, D. OpenID 2.0: A platform for user-centric identity management. In *Proceedings of the Second ACM Workshop on Digital Identity Management*, Alexandria, VA, USA, 30 Ocotber–3 November 2006; ACM: New York, NY, USA, 2006; pp. 11–16.
23. Berg, B.V.; Leenes, R.E. Audience segregation in social network sites. In Proceedings for Second IEEE International Conference on Social Computing/Second IEEE International Conference on Privacy, Security, Risk and Trust (SocialCom2010/PASSAT2010), Minneapolis, MN, USA, 20–22 August, 2010; pp. 1111–1117.
24. Anzelmo, E.; Bassi, A.; Caprio, D.; Dodson, S.; Kranenburg, R.V.; Ratto, M. *Discussion Paper on the Internet of Things*; Commissioned by the Institute for Internet and Society: Berlin, Germany, 2011.
25. Bassi, A.; Horn, G. *Internet of Things in 2020: A Roadmap for the Future*; European Commission: Information Society and Media: Brussels, Belgium, 2008.
26. Fritsch, L. State of the Art of Privacy-Enhancing Technology (PET)—Deliverable D.2.1 of the PET Web Project; No. 1013; Norsk Regnesentral: Oslo, Norway, 2007.
27. Pfitzmann, A.; Hansen, M. Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management—A Consolidated Proposal for Terminology; Technische Universität Dresden: Dresden, Germany, 2010.
28. Panurach, P. Money in electronic commerce: Digital cash, electronic fund transfer, and Ecash. *Commun. ACM* **1996,** *39*, 45–50.
29. Brands, S.A. Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy; MIT Press: Cambridge, MA, USA, 2000.
30. Camenisch, J.; Herreweghen, E.V. Design and implementation of the idemix anonymous credential system. In *Proceedings of the 9th ACM Conference on Computer and Communications Security*, Washington, DC, USA, 18–22 November 2002; ACM: New York, NY, USA, 2002; pp. 21–30.
31. Paquin, C. *U-Prove Technology Overview*; Version 1.1; Microsoft Corporation: Redmond, WA, USA, 2011.
32. Chaum, D. Security without identification: Transaction systems to make big brother obsolete. *Commun. ACM* **1985**, *28*, 1030–1044.
33. FIDIS (Future of Identity in the Information Society). *FIDIS Deliverable D3.1: Structured Overview on Prototypes and Concepts of Identity Management Systems*; FIDIS: Messkirch, Germany, 2005.
34. Rossnagel, H. The market failure of anonymity services. In *Information Security Theory and Practices. Security and Privacy of Pervasive Systems and Smart Devices*, Samarati, P., Tunstall, M., Posegga, J., Markantonakis, K., Sauveron, D., Eds.; Springer: Berlin, Germany, 2010; Volume 6033, pp. 340–354.
35. Rossnagel, H.; Zibuschka, J.; Pimenides, L.; Deselaers, T. Facilitating the adoption of Tor by focusing on a promising target group. In *Proceedings of the 14th Nordic Conference on Secure IT Systems: Identity and Privacy in the Internet Age*, Oslo, Norway, 14–16 October 2009; pp. 15–27.
36. Gideon, J.; Egelman, S.; Cranor, L.; Acquisti, A. Power strips, prophylactics, and privacy, oh my. In *Proceedings of the Second Symposium on Usable Privacy and Security*, Pittsburgh, PA, USA, 12–14 July 2006.

37. Fritsch, L.; Fuglerud, K.S.; Solheim, I. Towards inclusive identity management. *Identity Inf. Soc.* **2010**, *3*, 515–538.
38. Fuglerud, K.S. Universal design in ICT services. In *Inclusive Buildings, Products & Services: Challenges in Universal Design*, Vavik, T., Ed.; Akademika Forlag: Trondheim, Norway, 2009; pp. 244–267.
39. Fuglerud, K.S.; Reinertsen, A.; Fritsch, L.; Dale, Ø. *Universal Design of IT-Based Solutions for Registration and Authentication*; Norwegian Computing Center: Oslo, Norway, 2009.
40. Fritsch, L.; Abie, H. A road map to the management of privacy risks in information systems. In *Proceedings of Konferenzband Sicherheit*, Bonn, Germany, 2 April 2008; pp 1–15.
41. Fritsch, L.; Fuglerud, K.S. *Time and Usability as Upper Boundary in Friend and Family Security and Privacy*; DART/11/2010; Norsk Regnesentral: Oslo, Norway, 2010.
42. Fritsch, L. Security and privacy engineering for corporate use of social community platforms. In *Informatik 2011: Informatik schafft Communities, Beiträge der 41. Jahrestagung der Gesellschaft für Informatik e.V. (GI)*; Heiß, H.-U., Pepper, P., Holger, S., Schneider, J., Eds.; Gesellschaft für Informatik (GI): Berlin, Germany, 2011.
43. Ashton, K. That "Internet of Things". Available online: http://www.rfidjournal.com/article/view/4986 (accessed on 6 January 2012).
44. Zanero, S.; Savaresi, S. Unsupervised learning techniques for an intrusion detection system. In *Proceedings of ACM Symposium on Applied Computing*, Nicosia, Cyprus, 14–17 March 2004; pp. 412–419.
45. Hildebrandt, M. Trusted e-services for the citizen. Presented at *ICT Conference 2010*, Lyon, France, 10–11 February 2010.