Universidade de Aveiro Departamento de Eletrónica,
Telecomunicações e Informática
2015

**João Miguel
Ribeiro Gonçalves**

Privacidade em Comunicações de Dados para Ambientes Contextualizados

Context-awareness Privacy in Data Communications

Universidade de Aveiro Departamento de Eletrónica,
Telecomunicações e Informática
2015

**João Miguel
Ribeiro Gonçalves**

Privacidade em Comunicações de Dados para Ambientes Contextualizados

Context-awareness Privacy in Data Communications

"*By always being visible, by constantly living under the reality that one could be observed at any time, people assimilate the effects of surveillance into themselves. They obey not because they are monitored but because of their fear that they could be watched.*"

— **Daniel J. Solove** in *The Digital Person*

Universidade de Aveiro
2015

Departamento de Eletrónica,
Telecomunicações e Informática

João Miguel
Ribeiro Gonçalves

Privacidade em Comunicações de Dados para Ambientes Contextualizados

Context-awareness Privacy in Data Communications

Dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Doutor em Informática pelas Universidades do Minho, Aveiro e Porto (MAP-i), realizada sob a orientação científica do Doutor Rui L. Aguiar, Professor catedrático do Departamento de Eletrónica, Telecomunicações e Informática da Universidade de Aveiro, e do Doutor Diogo Gomes, Professor auxiliar do Departamento de Eletrónica, Telecomunicações e Informática da Universidade de Aveiro.

Work partially supported by PT Inovação.

Work partially supported by the European Commission via FP7 SOCIETIES project (No. 257493).

Dedico este trabalho à Inha, tendo a consciência que é apenas uma fração do que me dedicou a mim.

o júri / the jury

presidente / president

Doutor Vitor José Babau Torres
Professor Catedrático da Universidade de Aveiro

vogais / examiners committee

Doutor Rui Luís Andrade Aguiar
Professor Catedrático da Universidade de Aveiro

Doutor Rui Carlos Mendes Oliveira
Professor Associado da Universidade do Minho

Doutor Paulo Alexandre Ferreira Simões
Professor Auxiliar da Faculdade de Ciências e Tecnologia da Universidade de Coimbra

Doutor André Ventura da Cruz Marnoto Zúquete
Professor Auxiliar da Universidade de Aveiro

Doutor Artur Hecker
Maître de conférence na *Télécom ParisTech*
Diretor da *Future Networks Technologies, European Research Center, Huawei Technologies*

agradecimentos / acknowledgements

I would like to start by thanking my supervisors, Rui Aguiar and Diogo Gomes, for their guidance, lessons and straightforwardness. A special thanks to Diogo for all I learned from him even before he became my co-supervisor. Also a word to other members in the ATNoG research group, namely Mário Antunes for the discussions, and André Raínho and João Paulo Barraca for technical support.

I would like to thank my colleagues from the SOCIETIES project, which were the best ones I could have for openly discussing with and supporting the implementation of my ideas in the project. Among all, I owe special thanks to Alec Leckey, Eliza Papadopoulou, Nicolas Liampotis, Olivier Maridat and Miquel Martin.

Although the following thanks are frequently delivered directly, I'd like to publicly recognize the key role that my life-long friends and fellow techies Ricardo Otero, Tiago Pinto and Rui Ramos play in my culture and perspectives. Although they are absolutely non-academic, I could hardly wish for more interesting and savvy friends.

I would also like to thank my colleagues from PT Inovação that have helped me in my professional and personal paths throughout these years, namely Filipe Pinto, Telma Mota, José Albergaria, Nuno Pássaro, Nuno Carapeto, Pedro Santos, Christopher Viana and Sancho Rêgo. Also a special thanks to Luís Miguel Silva for personifying the company's support of this work.

Finally, I thank my family for the opportunity to do this work and for all the confidence and love they bless me with. I thank all my friends for colouring my life, especially two groups: os Índios and a República. They are an essential part of my motivation for doing scientific work as they stubbornly keep restoring my faith in humanity.

Palavras Chave

privacidade, informação pessoal, informação de contexto, identidade, sistemas distribuídos, análise de dados, anonimidade, sensores, publicidade na internet, redes sociais

Resumo

Quem usa a Internet vê publicidade direccionada com base nos seus hábitos de navegação, e provavelmente partilha voluntariamente informação pessoal em redes sociais. A informação disponível nos novos telemóveis é amplamente acedida e utilizada por aplicações móveis, por vezes sem razões claras para isso. Tal como acontece hoje com os telemóveis, no futuro muitos tipos de dispositivos elecónicos incluirão sensores que permitirão captar dados do ambiente, possibilitando o surgimento de ambientes inteligentes. O valor dos dados captados, se não for óbvio, pode ser derivado através de técnicas de análise de dados e usado para fornecer serviços personalizados e definir estratégias de negócio, fomentando a economia digital.

No entanto estas práticas de recolha de informação criam novas questões de privacidade. As práticas naturais de relações inter-pessoais são dificultadas por novos meios de comunicação que não as contemplam, os problemas de segurança de informação sucedem-se, os estados vigiam os seus cidadãos, a economia digital leva á monitorização dos consumidores, e as capacidades de captação e gravação dos novos dispositivos eletrónicos podem ser usadas abusivamente pelos próprios utilizadores contra outras pessoas.

Um grande número de áreas científicas focam problemas de privacidade relacionados com tecnologia, no entanto fazem-no de maneiras diferentes e assumindo pontos de partida distintos. A privacidade de novos cenários é tipicamente tratada verticalmente, em vez de re-contextualizar trabalho existente, enquanto os problemas actuais são tratados de uma forma mais focada. Devido a este fraccionamento no trabalho existente, um exercício muito relevante foi a sua estruturação no âmbito desta tese. O trabalho identificado é multi-disciplinar - da criptografia à economia, incluindo sistemas distribuídos e teoria da informação - e trata de problemas de privacidade de naturezas diferentes.

À medida que o trabalho existente é apresentado, as contribuições feitas por esta tese são discutidas. Estas enquadram-se em cinco áreas distintas: 1) identidade em sistemas distribuídos; 2) serviços contextualizados; 3) gestão orientada a eventos de informação de contexto; 4) controlo de fluxo de informação com latência baixa; 5) bases de dados de recomendação anónimas. Tendo descrito o trabalho existente em privacidade, os desafios actuais e futuros da privacidade são discutidos considerando também perspectivas socio-económicas.

Keywords

privacy, personal information, context information, identity, distributed systems, data mining, anonymity, sensors, online advertising, social networks

Abstract

Internet users consume online targeted advertising based on information collected about them and voluntarily share personal information in social networks. Sensor information and data from smart-phones is collected and used by applications, sometimes in unclear ways. As it happens today with smartphones, in the near future sensors will be shipped in all types of connected devices, enabling ubiquitous information gathering from the physical environment, enabling the vision of Ambient Intelligence. The value of gathered data, if not obvious, can be harnessed through data mining techniques and put to use by enabling personalized and tailored services as well as business intelligence practices, fueling the digital economy.

However, the ever-expanding information gathering and use undermines the privacy conceptions of the past. Natural social practices of managing privacy in daily relations are overridden by socially-awkward communication tools, service providers struggle with security issues resulting in harmful data leaks, governments use mass surveillance techniques, the incentives of the digital economy threaten consumer privacy, and the advancement of consumer-grade data-gathering technology enables new inter-personal abuses.

A wide range of fields attempts to address technology-related privacy problems, however they vary immensely in terms of assumptions, scope and approach. Privacy of future use cases is typically handled vertically, instead of building upon previous work that can be re-contextualized, while current privacy problems are typically addressed per type in a more focused way. Because significant effort was required to make sense of the relations and structure of privacy-related work, this thesis attempts to transmit a structured view of it. It is multi-disciplinary - from cryptography to economics, including distributed systems and information theory - and addresses privacy issues of different natures.

As existing work is framed and discussed, the contributions to the state-of-the-art done in the scope of this thesis are presented. The contributions add to five distinct areas: 1) identity in distributed systems; 2) future context-aware services; 3) event-based context management; 4) low-latency information flow control; 5) high-dimensional dataset anonymity. Finally, having laid out such landscape of the privacy-preserving work, the current and future privacy challenges are discussed, considering not only technical but also socio-economic perspectives.

Contents

List of Figures

List of Tables

Glossary

AmI	Ambient Intelligence
API	Application Programing Interface
CA	Certification Authority
CxB	Context Broker
CxC	Context Consumer
CxMA	Context Management Architecture
CxP	Context Provider
CxS	Context Source
DA	Domain Authority
DNS	Domain Name System
DNT	Do Not Track
EU	European Union
FIPs	Fair Information Practices
FTC	Federal Trade Commission
GPS	Global Positioning System
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICT	Information and Communication Technologies
IETF	Internet Engineering Task Force
IM	Instant Messaging
IdM	Identity Management
IdP	Identity Provider
IOI	Items-Of-Interest
IoT	Internet of Things
IP	Internet Protocol
LBS	Location-Based Services
M2M	Machine-to-Machine Communications
MitM	Man-in-the-Middle
MIS	Management Information Systems
MOM	Message-Oriented Middleware
NSA	National Security Agency
OASIS	Organization for the Advancement of Structured Information Standards
OECD	Organisation for Economic Co-operation and Development
OTR	Off-The-Record communication
P3P	Platform for Privacy Preferences
PETs	Privacy-Enhancing Technologies
PGP	Pretty Good Privacy
PPDM	Privacy-Preserving Data Mining
PKI	Public Key Infrastructure
PAP	Policy Administration Point
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PIP	Policy Information Point
PIR	Private Information Retrieval
PubSub	Publish-Subscribe
QoC	Quality of Context
REST	Representational State Transfer
RFID	Radio-Frequency Identification
SAML	Security Assertion Markup Language
SDB	Statistical Database
SDC	Statistical Disclosure Control
SMC	Secure Multi-party Computation
SSH	Secure Shell
SSL	Secure Socket Layer
SSO	Single Sign-on
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TTP	Trusted Third-Party
VANET	Vehicular Ad-hoc Network

US	United States
XACML	Extensible Access Control Markup Language
XEP	XMPP Extension Protocol
XML	Extensible Markup Language
XMPP	Extensible Messaging and Presence Protocol

Chapter One

Introduction

1.1 Background

When the Internet started being accessible to the general public there were little incentives and tools to share information online. Chat-room users perceived the Internet a world separated from the “real” one, where they went by awkward *screen names* and managed their privacy towards other users by slowly disclosing facts but also through feeding false information. Today’s real-name online social networks obsoleted the privacy tactics of the past. While some information and public image management is possible, the norm has become that people subject themselves to high levels of exposure in mainstream social networks. A comparatively small number of internet users, that wish to communicate without exposure, seek refuge in anonymous bulletin boards such as 4chan [Poole 2010]. Even simple web browsing is tracked and used to profile user preferences for targeted advertising. If in the Internet of 20 years ago nobody knew you were a dog (Figure 1.1), today your dog food is pictured on Instagram, *liked* on Facebook and suggested in an Gmail ad.

The Internet is changing from a separated world to a digital representation of the off-line world. Online social networks increasingly portray face-to-face social relations [Madden et al. 2013], and the interface with traditional entities such as banks, governments and retailers is increasingly done through the web. As connectivity reaches everywhere and electronic devices become smaller, the Internet is bound to become part of the physical world, integrated with it in every way possible [Punie 2003]. The change in paradigm will lead to another change in the privacy norm, predictably in the same direction: greater exposure for most people and a minority aggregating in a dark corner of the Internet where creativity thrives together with illegality and unaccountability.

P. Steiner
“On the Internet, nobody knows you’re a dog.”
©The New Yorker Collection 1993 Peter Steiner
From cartoonbank.com. All rights reserved.

Figure 1.1: Popular Internet-culture cartoon by Peter Steiner, published in *The New Yorker* in 1993

The work presented in this thesis started out as a more technical-oriented but, as it progressed, a multi-disciplinary approach became necessary to appropriately address the problem of privacy in future context-awareness scenarios. The variety of technical areas and perspectives on privacy harms depicts a fractured landscape that can only be understood if the socio-economical context is taken into account. In scientific terms, the contributions made in an area that so intricately influences users only has to gain from such a multi-disciplinary approach, both in terms of quality and relevance.

1.2 Motivation

1.2.1 Why Privacy Matters

One of the most common arguments against privacy is the *nothing to hide* argument. Famously, Google CEO Eric Schmidt stated in an interview to CNBC [Esguerra 2009]:

> If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place.

The argument is commonly phrased as a question such as "If you've got nothing to hide, then what do you have to fear?" and can be compelling when framed within a legality context, suggesting that only people that desire to conceal unlawful activity should be concerned [Solove 2007, p. 751]. The main fallacy of the argument is the narrow conception of privacy it considers, equating it to simply "hiding a wrong" [Schneier 2006], disregarding its other dimensions such as intimacy [Solove 2007, p. 764]. Furthermore, the argument ignores the cases in which privacy is threatened not by a singular well-defined act, but by a slow series of relatively minor ones [Solove 2007, p. 769].

In order to better illustrate the value of privacy, let us understand the implications of its absence. The *Panopticon* is an architectural design for a prison, originally conceived by Jeremy Bentham in the 18th century. A panopticon consists of an annular building with a tower at the centre and cells at the periphery. Prisoners are allocated individually to each cell and are perfectly observable from the tower due to the effect of back-lighting. Due to its design, with a central observation tower from which all prisoners can be observed while concealing if they are being watched at a given time, the surveillance effect becomes extremely more effective. By living under a reality in which one could be observed at any time, people assimilate the effects of surveillance into themselves [Solove 2004, p. 30].

The kind of power that privacy deprivation brings is well illustrated by the Panopticon. It forces individuals to live in constant fear of external scrutiny, behaving conservatively regarding their own perception of the judgement that observers will make of their actions. Similarly to the *telescreen* from George Orwell's *Nineteen Eighty-Four*, the Panopticon enables social control and suppression of individuality [Solove 2004, p. 32]. Privacy is necessary for self-evaluation and self-definition. It enables individuals to separate themselves from others and negotiate what to share and to keep for themselves [Kerr, Steeves, and Lucock 2009, p. 205]. As illustrative examples of the close relation between privacy and individuality, the jurisprudence developed in Germany and Switzerland regarding privacy and data protection has at its centre the concepts of *Persönlichkeitsrecht* and *Persönlichkeitschutz*, which translate to the protection of personality [Bygrave 2010, p. 169].

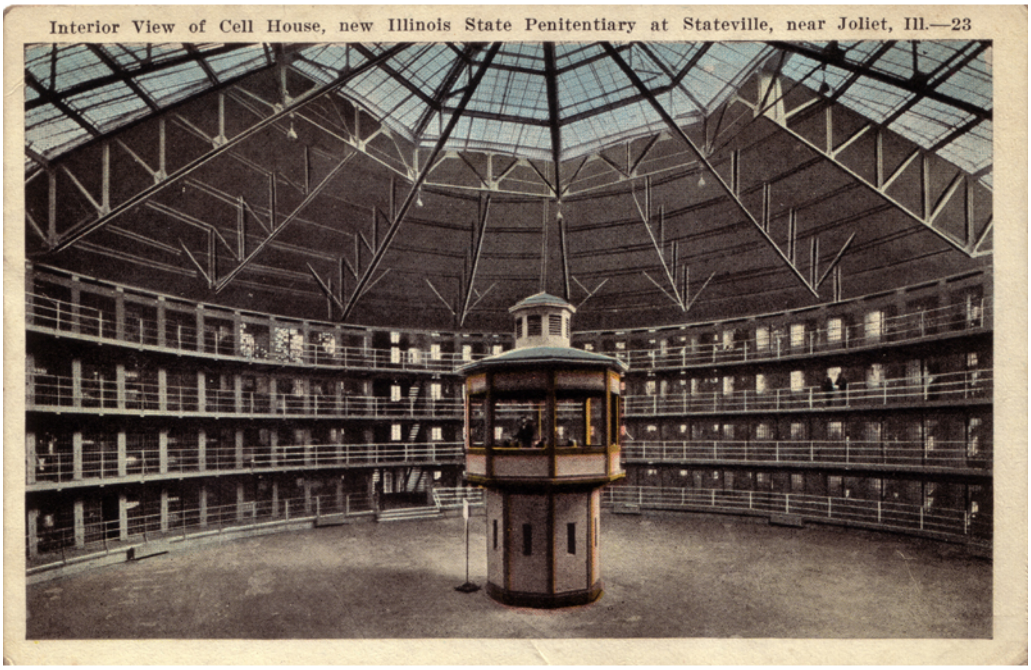
Interior View of Cell House, new Illinois State Penitentiary at Stateville, near Joliet, Ill.—23

Figure 1.2: Postcard of an American panopticon, retrieved from [Wellerstein 2013]: “Interior view of cell house, new Illinois State Penitentiary at Stateville, near Joliet, Ill.”

Privacy is also a key requirement for democratic health. Again Germany, a country commonly cited has having the most privacy-friendly laws in the world, clarified through its Constitutional Court the key value of data protection with respect to securing the necessary conditions for active citizen participation in public life [Bygrave 2010, p. 172]. If privacy is not protected, political control could be exerted even before political movements become democratically relevant, by monitoring and disrupting association and self-determination.

1.2.2 Zeitgeist

Historically, there are a few key definition moments for privacy. The most relevant so far took place in the 1970s, when most of the privacy concepts currently in use were developed. After some decades of low attention, privacy is now back in the spotlight. There are three main motives that can explain why privacy re-emerged as a popular topic for public discussion: government surveillance, the digital economy and the current moment of technological development.

The publication of proof that the National Security Agency (NSA) conducts mass surveillance programs [Greenwald 2013] in 2013 was a key trigger for public discussion of privacy issues. On the table are a number of topics, such as whether mass surveillance is necessary for preventing terrorist attacks, and whether safety from terrorism justifies these practices. There are also fears of consumer backlash in the technological economy for the role that Internet enterprises and telecommunication operators play in the exposed intelligence gathering programs. However, the enterprises are not completely innocent in this.

The digital economy, that enables innovative enterprises to flourish and make available free Internet services, feeds on personal data. Targeted advertising, which builds user profiles based on browsing habits and social network preferences, represents the key source of revenue for web enterprises. The personal data aggregation performed is profitable for them, but it may also be for hackers, identity thieves or intelligence agencies. The privacy threats that tracking and profiling practices enable led the European Union (EU) to start the Data Protection reform in 2012. This reform aims to set *fair game* rules for personal data gathering and use practices by enterprises and governments. However, the process has been lengthy and problematic and is not likely to finish before 2016.

Technological development is a key motivator for privacy discussion. It was the trigger in the 1970s, as well as in 1890, which led to the definition of privacy as the *right to be let alone.* The popularization of social networking sites in recent years also motivated some privacy discussion prompted by questionable information sharing options and long term privacy risks. The problems caused by excessive personal sharing can go from mild embarrassment to serious professional and social problems. Currently, the latest technology products being questioned on the subject of privacy are the ones related to wearable computing and augmented reality, namely Project Glass from Google. As consumer-grade devices increasingly enable people to transparently gather, record and access more information, artificially augmenting human perception, the existing expectations of privacy will be challenged.

Given the current issues and ongoing public discussions, it's justifiable to consider that we currently are at another historic definition point for privacy.

1.3 Hypothesis and Objectives

When the goal is security, the problem is typically simplified through an attack model where the objective is to simply thwart the attack under a given set of assumptions. When privacy is addressed, it's difficult to come up with such a simplification that allows us to have only one objective without abstracting away essential parts of the problem. Embedded in the very concept of privacy, there is a notion of trade-off and choice. From an individual point of view, privacy involves choices between transparency and reserve, publicity and discreteness, that are highly context dependent and sometimes even apparently inconsistent [Acquisti 2009]. From a societal point of view, privacy choices are equally complex. As technological development will lead to increased communication and accessibility, more technology generally equates to less privacy. It should be of concern to technologists that their work benefits society while minimizing privacy threats, optimizing the overall social outcome of scientific and technological development.

Surveillance techniques are argued to provide improved protection from terrorism and crime, but they also raise democratic concerns of different natures. The most common concerns involve Orwellian *Big Brother* scenarios, where governments exerts totalitarian control over the population suppressing individualism and political dissidence. Another recent concern, which also threatens essential freedoms and the rule of law, is better illustrated by Franz Kafka [Solove 2004]. In *Der Prozess* Kafka describes an excessively bureaucratic faceless organization that holds an unbounded amount of data about individuals. This organization takes decisions about individuals without adequate accountability or justification, disregarding individual's right to a fair trial. Such problems can easily arise from the adoption of automated investigation and population profiling mechanisms [Solove 2004, p. 180]. While in an Orwellian scenario there is an intention to control the population, in a Kafkian scenario the disrespect for essential freedoms is a by-product of an over-powered bureaucratic poorly accountable state.

Another privacy dilemma has to do with trade-offs between human comfort provided by services which live off the digital economy and the threats that arise from excessive aggregation of information by enterprises that provide such services. Innovative Internet services and mobile applications, usually available free of charge to users, are very appealing from both individual and societal perspectives. However, the hidden cost is, in best case scenario, generalized consumer profiling. More obscure cases involve detailed individual profiling for business intelligence and direct marketing and questionable data transactions that can enable criminal activities such as identity theft [Krebs 2013].

At the moment, science and technology are not well equipped to deal with these dilemmas. Privacy has been addressed in a fragmented way, separately addressing techniques and future use cases. The work developed from each viewpoint has seldomly established links to work developed in other disciplines. A comprehensive structuring review of the key efforts in each of the numerous privacy-relevant areas needs to be done before privacy is tackled as a core objective, instead of being a supposed consequence of security.

Aiming to address these topics, the hypothesis of this thesis states: unidentified synergies between different privacy-related bodies of knowledge exist that are key for improving privacy in face of near-future technologies. Given the multi-dimensional nature of privacy, multi-disciplinary work is necessary in order to appropriately address privacy trade-offs, and to maximize the social outcome of technological progress. Consequently, the work presented in this thesis considers privacy from a variety of perspectives, mostly technical but also social, economical and political. The concept of privacy is explored drawing mostly from the legal field, and the diverse existing technical privacy-related bodies of knowledge are analysed and inter-related. The areas that focus on communication - for control of data flows and identifiers - and data analysis - enabling evaluation of the potential privacy harm - are given special attention. Considering the vision of Ambient Intelligence (AmI) for the near future, this thesis also addresses the privacy challenges derived from the widespread implementation of context-awareness. The conclusion identifies and presents work in a number of promising research tracks that effectively address privacy issues applicable to a variety of future use cases, and formulates recommendations for resolving the current privacy dilemmas.

1.4 Contributions

The contributions to the state-of-the-art done in the course of the work presented in this thesis fit essentially in two fields: Context Management and Privacy-Preserving Data Mining (PPDM) . However there has also been significant analysis and implementation effort towards building an identity layer for use in the European Project Societies, described in Section 3.3.5, which resulted in a prototype [SOCIETIES 2011], a communication, derived research and a conferece publication [Gonçalves and Gomes 2014].

Contributions in Context Management were done in different steps. The earliest contributions focus on two possible future applications, as well as the service-oriented implementations of these applications. One of them performs content selection based on context information instead of using traditional recommender techniques [Gonçalves, Delahaye, and Lamorte 2010]. The other consists of a triggering system based on event occurrence which can be used in different use cases with different business models [Simões et al. 2009]. These contributions were done based on an early contribution in area of context management [Zafar et al. 2009]. The next step was a contribution towards event-based context management, enabling real-time adaptation of services [Gomes et al. 2010] and a fine-grained access control mechanism that respects the real-time constraints of such system [Gonçalves, Gomes, and Aguiar 2012].

In the field of PPDM, the contribution was a dataset sanitization technique, inspired in communications-related privacy work such as pseudonyms and Identity Management (IdM) . The technique works in high-dimensional datasets where most techniques fail, while preserving dataset utility for recommendation, the most common data mining objective for such datasets. This opens the possibility of further work combining the IdM and PPDM fields, establishing the missing link between data management in the IdM perspective and in the data analysis and aggregation perspective. The final goal of this work track would be making IdM resistant to data-level re-identification while maintaining partial identity profiling for recommendation and other benefits of data mining.

The list of publications and communications relevant to the work presented in this Thesis is presented in Table 1.1. Central to it, but only superficially communicated in a national event, is the structured analysis of privacy problems and existing solutions done in this thesis, and the multi-disciplinary approach that enables better understanding and framing of privacy issues and technologies. Finally, the socio-economical and technical review and discussion of the current privacy landscape is exclusively published in this thesis, including an analysis of privacy topics addressed in mass media, drawn from the tags of thousands of privacy-related news published over the last 30 years. The discussion addresses current social dilemmas and economic incentives, as well as the technological and legal responses to privacy issues, synthesizing the moment and giving a future outlook on how these issues can evolve.

Table 1.1: List of Publications and Communications

Year	Type	Title	Target
2009	Conference	Context Management Architecture for Future Internet Services	ICT Mobile and Wireless Communications Summit 2009
2009	Conference	CATS: Context-Aware Triggering System for Next Generation Networks	IFIP Advances in Information and Communication Technology: Wireless and Mobile Networking
2010	Conference	Professional and User-Generated Content Rating using Context Information	Networked & Electronic Media Summit 2010
2010	Conference	XMPP based Context Management Architecture	2010 IEEE Globecom Workshops
2011	Communication	Societies Positions on Federated Social Networking	W3C Federated Social Web Summit Europe 2011
2012	Conference	Low-latency privacy-enabled Context Distribution Architecture	2012 IEEE International Conference on Communications (ICC)
2013	Communication	Privacy Untangled	17o Seminário da Rede Temática de Comunicações Móveis (RTCM)
2014	Conference	User-Hosted SOA Infrastructure over XMPP	2014 IEEE Symposium on Computers and Communications

1.5 Structure

This thesis has at its core three technical chapters, separated according to the fields they cover. These are surrounded by multi-disciplinary chapters: the ones preceding define and frame the work, and the ones finalizing to analyse impact and outlook the future.

Chapter 2 sets the ground for working on privacy: its definition, importance, history and relation with ICT, as well as current foreseeable future threats. A survey of privacy technologies is presented in Section 2.3, structuring them according to their academic field or practical applications.

Each of the three technical chapters focuses a different set of fields, aggregated by their general area. Chapter 3 addresses privacy from a communications and distributed systems point of view, addressing network and transport, identity and access control issues. Then, Chapter 4 focuses on future context-awareness scenarios which build upon communication technologies to provide service and environment adaptation. Finally, Chapter 5 addresses privacy from a data point of view, focusing on re-identification and other privacy issues created by current data aggregation and mining practices.

In the two final chapters, having proposed a number of contributions to enhance privacy, a multi-disciplinary analysis is presented where these contributions are framed and identifying additional key research paths and public discussion topics. In Chapter 6 ICT-motivated privacy issues are revisited from four different perspectives: social, economic, technological and legal. Finally, in Chapter 7, the thesis is concluded by synthesizing results, showing the way for future privacy research and laying out a set of recommendations towards a socially-profitable technologic evolution, with regards to privacy.

Chapter Two

Privacy in ICT

The landscape of privacy issues related to technology is described, as well as areas of scientific work aiming to address them. This exercise aims to structure privacy-related work, which is often multi-disciplinary and developed under very different assumptions, and also frame the work presented in this thesis.

2.1 Introduction

2.1.1 Chapter Outline

In technology, privacy is studied in distinct fields under different assumptions to tackle different problems. A number of bodies of knowledge target overlapping parts of privacy, which are bound to be relevant for current and future technology-caused privacy issues. However a holistic and consistent view of privacy-related knowledge requires a well-defined overarching conceptual framework for privacy, which is possible to gather mostly from non-technological disciplines. For that reason, this Chapter starts by contextualizing privacy, and moves on to provide an overview of existing privacy definitions drawing from work in several fields in Section 2.2. Then, in Section 2.3 an overview of the plentiful and disparate technology and privacy relevant bodies of knowledge is given.

2.1.2 A Human Right

First and foremost, privacy is a human right according to two post World War II international agreements, which are among the most relevant agreements ever signed: the Universal Declaration of Human Rights and the European Convention on Human Rights.

> Article 12. No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.
>
> Universal Declaration of Human Rights

> Article 8 - Right to respect for private and family life
>
> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.
>
> European Convention on Human Rights

However these fundamental and consensual guarantees are formalized in different ways by different countries. As referred in Section 1.2, German privacy protection legislation emphasises its societal perspective, privacy as a requirement for active citizenship and free democratic participation [Bygrave 2010, p. 172]. This contrasts with the United States (US) privacy culture, in which privacy tends to be described as an individual right that can be in tension or against the needs of society [Bygrave 2010, p. 171]. The fact that the Fourth Amendment of the US Constitution, which protects against unreasonable searches and seizures, is often considered a key piece of US privacy legislation, illustrates this cultural difference quite well. The Fourth also applies to electronic eavesdropping since the US Supreme Court decision *Katz vs United States* in 1967 [Solove 2004, p. 198], but it only safeguards against privacy abuses committed by law enforcement and the government.

Despite these differences, legislation and regulation work worldwide have made most relevant contributions to the definition and safeguard of privacy. As introduced in Section 1.2, this has frequently been motivated by technological advances and media attention. In the past few years years there were plenty of news of surveillance programs of intelligence and security agencies, hacked consumer information databases and social networking sites privacy issues and mishaps. Looking beyond the current moment, technology and privacy also have a significant common history. Email privacy has been addressed since the 1980's [Chaum 1981], legal academic work in technology-related privacy issues has been around since mainframes began being used for storing personal information in the 1970's [Westin and Baker 1972], and privacy concerns stemming from technological progress date back to the popularization of photographic *snap cameras* more than 100 years ago [Warren and Brandeis 1890]. With technological development aiming to realize ever more connected visions, such as AmI, Internet of Things (IoT) and Machine-to-Machine Communications (M2M) , ICT-motivated privacy issues are bound to become even more relevant in the near future.

2.1.3 Historical Perspective

At the end of the nineteenth century, Warren and Brandeis [1890] formulated the right to privacy as the *right to be let alone*. What prompted them to do this was the introduction of the *snap camera* by Kodak, a hand-held camera that could take photographs at the click of a button, commercialized with the adequate advertising slogan *You Press the Button, We Do the Rest*. In *The Right to Privacy*, Warren and Brandeis noted that, with this new technology, pictures could be taken without the photographed individual being required to stand still and pose, and argued for new legislation to prevent pictures to be taken without permission:

> Now that modern devices afford abundant opportunities for the perpetration of such wrongs without any participation by the injured party, the protection granted by the law must be placed upon a broader foundation.

The 1970s were a very relevant decade for the protection of privacy, with respect to the collection and use of personal data enabled by technological advancement. In 1972, *Databanks in a Free Society* [Westin and Baker 1972] highlighted how the use of mainframe computers of the time for the purposes of record keeping enabled privacy harms. Although the book is largely outdated, it argued that a citizen must have the right to access data records that refer to them. The following year a US government report [W. H. Ware 1973] argued for the creation of a set of Fair Information Practices (FIPs) , required to "establish standards of record-keeping practice appropriate to the computer age". Subsequent work developed these FIPs which where applied to federal agencies in the US with the Privacy Act of 1974. Around that time European countries began to enact privacy laws applicable not only to the public but also to the private sector, namely Sweden, the Federal Republic of Germany, and France [Gellman 2013]. At the end of the decade the Organisation for Economic Co-operation and Development (OECD) presented the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* [Organisation for Economic Co-operation and Development 1980], which was the first international regulation effort on the matter. Although the FIPs were drafted in the '70s it was not until 2000 that the Federal Trade

Commission (FTC) published them as a regulatory framework for private entities in the US [Federal Trade Commission 2000; Gellman 2013].

On the technological perspective of privacy protection, the '70s also were relevant, especially regarding the development of encryption techniques. Public-key cryptography was introduced in 1978 with the RSA paper [Rivest, Shamir, and Adleman 1978]. In 1981 Chaum proposed a mechanism to anonymously send messages over an unsecure network without the need of a central trusted authority, using public-key cryptography [1981]. The paper coined the use of the term *mixes* to designate email anonymizer servers, or anonymous remailers. The posterior development and implementation of these remailers occured related with the *cypherpunk* movement, a tech-savvy activist group advocating for the widespread use of cryptography and other Privacy-Enhancing Technologies (PETs) . A decade later, the *Cypherpunk Manifesto* [Hughes 1993] argued that privacy in an open society requires anonymous electronic transaction systems, like physical money, and that such privacy requirements must be achieved by technical means, such as cryptography. Like other forms of activism, cypherpunks opposed the *status quo*, and consequently did not trust governments nor corporations with matters of privacy protection. Despite these actions, decades later, only a few of the acclaimed PETs are widely deployed. As an example, while the use of communication encryption became widespread with SSL and TLS, technologies that enable communication anonymity, such as mixes, have met significant implementation resistance [Goldberg 2007].

Ironically, what became widespread instead was the use of the Internet in a centralized way, where web service providers hold large ammounts of users' data in their databases. The accumulation of personal data by online service provides provided fertile ground for privacy issues to flourish. In 2006 AOL released search query data of 657 thousand anonymous users which was intended to be used for academic purposes. However, as a result, many users were quickly re-identified due to the specificity of the data, which included very sensitive queries such as "fear that spouse contemplating cheating" and "how to kill oneself by natural gas" [Barbaro and Jr 2006]. Another problematic data release was the Netflix Prize, a data mining competition that took place from 2007 to 2009. Netflix provided an anonymized dataset which the public would use to create better data mining algorithms for movie recommendations. The initiative was well received by the data mining community, but as Netflix announced a follow up competition in 2010, the FTC advised against it [Federal Trade Commission 2010], weary of potential privacy infringements after researchers managed do re-identify users of the Netflix dataset [Narayanan and Shmatikov 2008].

Careless data releases aren't only one type of issue raised by the accumulation of personal data. As the user-bases of online and telecommunication services grow, the value of their databases does as well, as do the security risks associated with maintaining them. In 2011, as a result of an hacking attack, Sony announced that personal information about Playstation online account holders, including names, addresses, e-mail addresses and possibly credit card numbers, could have been compromised [Bilton and Stelter 2011]. Furthermore, the value of personal data is not only appreciated by outlaws but also by governmental agencies. In April 2013 the US Foreign Intelligence Surveillance Court ordered Verizon, a major telecommunications company in the country, to daily provide the NSA with information regarding all phone calls that the operator serves, namely the numbers of both parties, location data, call duration, unique identifiers, and the time and duration [Greenwald 2013]. Other major american tech companies, namely Google, Facebook, Twitter, Microsoft and Apple, also have to provide user data on request to the NSA [Miller 2013b]. These two reports are part of the well-known “Snowden leaks”.

2.1.4 Privacy Legislation and the Digital Economy

The accumulation of personal data by companies did not occur accidentally: the value of personal information for economy has been recognized in the US for decades. In the 1970s the application of the FIPs was restricted to federal government agencies. For the private sector the US enacted the Fair Credit Reporting Act, a set of rules coherent with the FIPs, to regulate the practices of consumer reporting agencies that collect and compile consumer information into reports for use by credit grantors, insurance companies, employers, landlords, and other entities in making eligibility decisions affecting consumers [Federal Trade Commission 2011]. Nowadays the so-called digital economy orbits around personal information. Online targeted advertising is an established billion dollar market which provides most of the revenue for online service providers [Schonfeld 2009]. User’s browsing actions are tracked, typically by the use of *cookies*, and aggregated to build a profile that can be used for targeting ads. The microblogging giant Twitter had an advertising revenue of 269 million US dollars, but also had a *data licensing* revenue in 2012 of 47 million [Twitter Inc. 2013, p. 71]). The second item in their revenue sheet, data licensing, refers to another way of monetizing personal data, in this case *tweets*: selling or licensing the data to third parties. Companies that primarily focus the personal data selling business are usually denoted *data brokers*. One such company, Acxiom, collects, analyses and sells consumer information for use in business intelligence, having reported sales of 1130 million dollars in 2011 [Singer 2012]. Another such company, Experian, allegedly sold consumer data to a rogue site, *superget.info*, known for supplying data to identity thieves [Krebs 2013]. The privacy-related regulation of this market in the US is currently done by the FTC, which global mission is to act upon unfair or deceptive acts or practices in or affecting commerce. However, the FTC enforcement of the FIPs has been rather weak and reactive [Solove 2004, p. 72], and even some of the FIP-coherent regulation is considered not to adequately protect consumer interests, such as the Fair Credit Reporting Act which sets low hurdles for credit bureaus and insulates them from liability for defamation, invasion of privacy, and negligence [Harper 2005].

In Europe the scenario is somewhat different as, historically, privacy laws make little distinction whether personal information is being collected and used by a public or private entity [Gellman 2013, p. 5]. At the supra-national level, privacy started being addressed in 1995, by the EU, with Directive 95/46/EC, which attempts to enable the flows of personal information between EU member states as long as some FIPs are respected, namely legitimacy and transparency of data collection, confidentiality and security of data processing and liability of stored data. Two years later, the telecommunications sector privacy practices were targeted by EU Directive 97/66/EC, which defines mandatory security principles and limits to data retention. Directive 2002/58/EC generalizes the previous one from telecommunications to all electronic communications, and specifies security and confidentiality requirements applicable to communications and location data, as well as limits to spam. Subsequent directives 2006/24/EC and 2009/136/EC amend it with regards to data retention and web browser cookies consent requirements, respectively. Motivated by the the lack of European competition to the American digital economy, by legal discrepancies between EU member country privacy laws, and by citizen privacy concerns with privacy practices of Internet companies, the European Commission initiated in 2013 the EU Data Protection reform. The initiative included a EU Regulation for the general provisions applicable to public and private sectors and a Directive targeting criminal investigation authorities.

2.2 Defining Privacy

2.2.1 Different Views of Privacy

The different understanding that American and European legislators have regarding privacy has been introduced in Section 2.1.2. In the US privacy is primarily seen as liberty and protection from an abusive state, in the spirit of the Fourth Amendment. In turn, the private sector is subject to a set of regulatory practices and tort law. In Europe privacy is seen as a right which needs protection against any entity, public or private. However this is only one of the many different dimensions of possible interpretations regarding the term *privacy.* Most of privacy issues described in the historical outline of the previous section have strikingly different natures. The only thing they have in common is the fact that there is ICT and personal information involved, and that they are communicated using the same over-arching concept. As Solove puts it it in his work *A Taxonomy of Privacy* [2006, p. 485]:

> The term “privacy” is an umbrella term, referring to a wide and disparate group of related things.

Different scholar communities see very different perspectives of privacy. In an extensive interdisciplinary survey for use in Management Information Systems (MIS) Smith et al. categorized four distinct approaches to the study of privacy [Smith, Dinev, and H. Xu 2011]:

- Privacy as a Right, absolute, essential for a free and democratic society - an approach taken mostly by law scholars;
- Privacy as a commodity, subject to cost-benefit analysis and personal choice - mostly seen in economy and MIS;
- Privacy as a state, both physical and psychological, which enables reflexive processes - related to sociology and philosophy;
- Privacy as control, of information and exposure - observed in several areas, especially MIS and US law.

In this Section the definition of privacy is explored, drawing mostly from the legal field, where this matter was most addressed.

2.2.2 From Social Functions to Control of Information

Alan Westin passed away recently, at the age of 83, as one of the most cited authors for framing privacy-related work. In his 1967 book, *Privacy and Freedom* [1968], Westin characterizes privacy as a confusing and vague concept but puts forward a privacy definition widely used in modern work on privacy issues, in various fields of study. Westin formulates:

> Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.

However, another law scholar with significant contributions related to privacy, Daniel Solove, enumerates various authors focused on law and social sciences, many of them posterior to Westin, which note the complexity of the subject [2002, p. 1088] [2006, p. 479]. Furthermore he argues that proposed privacy definitions as a single overarching concept have consistently fallen short. Westin's definition is considered to be an information control formulation of privacy, which is only a subset of the privacy concept [Solove 2002, p. 1110] [Kerr, Steeves, and Lucock 2009, p. 192]. Despite this narrower result, an analysis on the psychosocial functions of privacy was included in *Privacy and Freedom* [Westin 1968]. Westin argues that privacy provides individuals and groups in society with a preservation of autonomy, a release from role-playing, a time for self-evaluation and for protected communication. He describes four basic states of individual privacy:

- solitude: the individual is separated from the group and freed from the observation of other persons;
- intimacy: the individual is a member of a small unit that claims and is allowed to exercise corporate seclusion so that it may achieve a close, relaxed, and frank relationship;
- anonymity: the individual is in public places or performing public acts but still seeks, and finds, freedom from identification and surveillance;
- reserve: the creation of a psychological barrier against unwanted intrusion.

Solitude is a state that represents isolation, allowing the individual release from social pressure and norms. This isolation does not limit itself to physical isolation and even includes psychological intrusion such as the strictness of one's conscience and the belief in an omniscient entity such as God. Solitude is a state for introspection, providing conditions for one to form his own identity and individuality. Intimacy is a state that responds to the need to be *off stage*. Still shielded from society's direct influence, it provides a trusted environment for interaction and sharing. The typical intimacy unit example is the Family, but its relevance has diminished in modern ages, being increasingly replaced with friendship relations. Other intimacy units are constructed and regulated by society, such as Attorney-client privilege and Physician-patient privilege. Anonymity and reserve, unlike solitude and intimacy, are privacy states observed in public environments. Anonymity is a state characterized by public action with accountability limited to its specific context. The individual does not expect to be personally identified and held to rules of behaviour other than those of the situational landscape he has merged into. The state of Anonymity only became possible with urbanization: while in small villages all individuals are known to each other, and if a stranger arrives he is identified as such, in the streets of a big city we are allowed to act within society's boundaries as though we are invisible. Finally, reserve is the state that comes into play in common interpersonal relations. It can be observed as the *reciprocal reserve and indifference* in social interactions in order to *protect the personality.*

Westin acknowledges the social nature of privacy in his work, however critique points out that this social dimension is undermined as the conceptualization work progresses [Kerr, Steeves, and Lucock 2009, p. 199]. He subsequently frames privacy under the assumption the individual is in conflict with the collective (i.e. society) regarding some disclosure issue. He formulates this conflict in terms of disclosure - the individual's choice of seeking out social interaction - and surveillance - social control that can be resisted by the individual. The focus on protecting the flow of information isolates the individual in the goal of privacy [Kerr, Steeves, and Lucock 2009, p. 200]. Under this formulation, absolute privacy comes from absolute seclusion.

2.2.3 A Practical Approach

In *Conceptualizing Privacy*, Solove [2002] questions the methodology to define privacy itself. He begins by showing unsatisfaction towards existing privacy formulations, which focus on finding a general and consistent formulation, and recognizes the multitude of meanings the term privacy can transmit:

> Currently, privacy is a sweeping concept, encompassing (among other things) freedom of thought, control over one's body, solitude in one's home, control over information about oneself, freedom from surveillance, protection of one's reputation, and protection from searches and interrogation.

Subsequently he argues that one could take a bottom up, more pragmatic, approach that would lead to fruitful understandings of privacy within specific contexts, rather than further add to the academic discourse on the common denominator of privacy. In his follow-up work, Solove [2006] proposes a taxonomy for use in privacy-related legislation so that it moves away from the vague term "privacy". As one would expect from his previous work, the approach taken focuses on the activities that may invade privacy and by how these are currently treated by the United States justice system. The result is a conceptualization of potentially harmful activities, categorized in four groups based on how they influence the data subject - the individual whose life is most directly affected by these activities.

1. Information Collection - focuses on disruption caused by data gathering activities, unrelated to the actual information collected:
   a) Surveillance - data gathering by observation possibly leading to self-censorship and inhibition, adversely impacting freedom, creativity, and self-development;
   b) Interrogation - data gathering by inquiry which typically involves coerciveness, frequently in disguise, creating discomfort even if information is barely disclosed.
2. Information Processing - focuses on issues that arise when already-collected data is handled:
   a) Aggregation - gathering together information about a person such that it becomes possible to compose a comprehensive portrait of that individual, even if he believes that in each information disclosure he is revealing relatively little;
   b) Identification - the association of data with a particular human being, which can increase biases and prejudices in data interpretation, as well as fear of reprisal in case the data is of political nature;
   c) Insecurity - issues in the way that information is handled or protected, that can lead to identity theft and subsequently to credibility and bureaucratic problems;

    d) Secondary Use - use of data for purposes unrelated to the purposes for which the data was initially collected, without the data subject's consent;
    e) Exclusion - failure to provide individuals with notice that a data record exists about him and to allow him to ensure that the information in said record is accurate.
3. Information Dissemination - focuses on harms caused by the revelation of personal data or the threat of spreading information:
    a) Breach of Confidentiality - release of privileged information by a trusted party, betraying the confidence of the data subject;
    b) Disclosure - release of true information that is potentially harmful to the data subject, namely in terms of his reputation and security;
    c) Exposure - exposing physical and emotional attributes about a person which may cause embarrassment and humiliation and that the normal social practice involves concealing (e.g. nudity and bodily functions);
    d) Increased Accessibility - make already publicly available information significantly more accessible such that it enhances its potential for harm;
    e) Blackmail - coercive control exercised over an individual by threatening to expose or disclose her personal secrets;
    f) Appropriation - use of the data subject's identity for the purposes and goals of a third party, colliding with the way the data subject desires to present herself to society, potentially interfering with her freedom and self-development;
    g) Distortion - inaccurate portrayal of a person to the public using false or misleading information, with the intention of manipulating the way a person is perceived and judged by others.
4. Invasion - focuses on privacy harms that don't always involve information
    a) Intrusion - Similar to Warren and Brandeis' *right to be let alone*: invasions or incursions into one's life that disturbs her daily activities and routines, destroys her solitude, and often makes her feel uncomfortable and uneasy;
    b) Decisional Interference - governmental interference with people's decisions regarding certain, private, matters of their lives.

Solove's taxonomy captures not only the information control perspective, but also emotional and social harms that relate to privacy, establishing links and relations between existing judicial elements such as laws, rulings and constitution articles, which address privacy issues. Nature of the activity, namely the goal of the data holder while performing it and its impact on the data subject, is the focus of the analysis. However, in the context of ICT, some of these activities are not especially relevant, while others are incredibly complex. As an example, while Appropriation and Distortion can be applified by the use of ICT, both from the exposure of the data subject and reach of data holder perspectives, they are essentially social activities. On the other hand, the great majority of Surveillance activities depend on the existence of ICT infrastructure, especially those which are more scalable and economically viable. In Section 6.5.2 the correspondence between privacy harming activities and technological issues is explored.

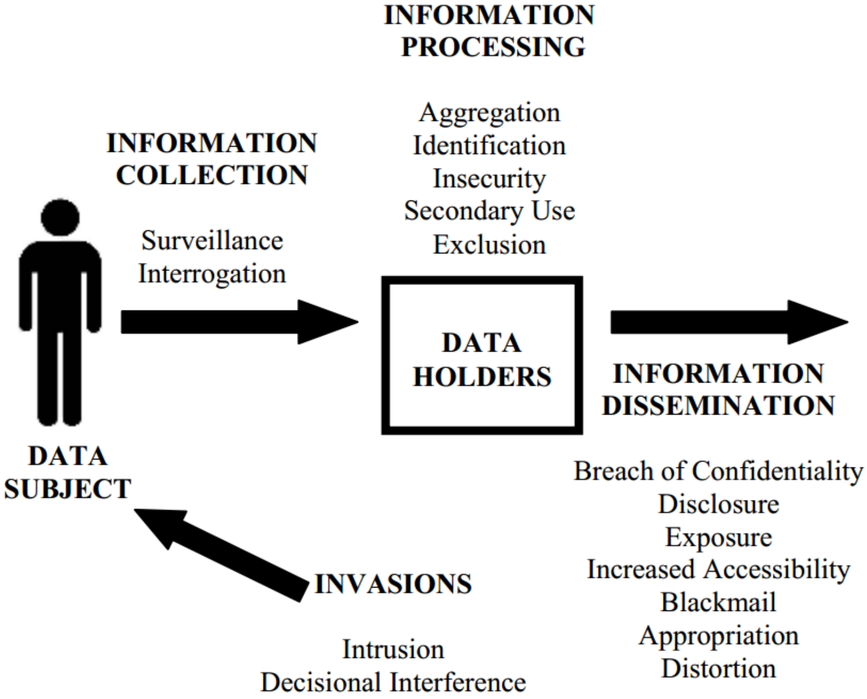

Figure 2.1: Privacy taxonomy figure from the original paper [Solove 2006]

2.2.4 Importance of Social Context

In the past, access to a personal or intimate information was mainly restricted by physical barriers (e.g. walls and closed doors). Traditional privacy expectations include temporal and spatial borders. These borders separate information from various periods or aspects of one's life. Also, a common assumption from oral communication practices is that interaction and communication are ephemeral, not to be captured or preserved through hidden video or audio [Marx 2001]. If such preservation is done, a conversation had in a specific situation can easily be re-interpretable in originally unintended ways, possibly decades after.

With the emergence of online commnication, information borders became significantly permeable. Social contexts are no longer bound by space and time as before. Behaviour cues given by online communication environments are often contradicting. The users struggle to transfer their naturally acquired social privacy practices to the online environments, often resulting in social awkwardness and embarrassment caused by disclosing information in a wrong context or using an unappropriate medium [Boyd 2002]. Social networking sites, more than their bulletin board predecessors, enable communication to a very wide audience. The bigger the audience and the types of information that can be shared, the more complex it becomes to manage privacy. Consider this well-known example: in 2010 Facebook had a privacy configuration of 50 settings and more than 170 options [Bilton 2010].

This complexity may be making the social networking giant a victim of it's own success. Three years after the *grandmother effect* on Facebook was announced [Wiggs

2010], the Pew Research Center reports that increasing adult presence in the social network has waned teenager enthusiasm for using it. Other social networking sites, such as Twitter and Instagram, are used because there teenagers are free social expectations and constraints of Facebook, and can better express themselves[Madden et al. 2013]. Instead of managing complex privacy settings, many teenagers simply choose another (digital) space for their interactions.

Despite these concerns, most teenagers keep an active Facebook account in order to not miss out, as it represents a key communication method. Also, they report high levels of confidence in managing privacy settings, as well as positive experiences online [Madden et al. 2013]. Managing privacy in new communication methods may be just a matter of cultural adaptation for the users and of improving user experience and managing the community for service providers.

Another key privacy issue with online sharing is its permanent nature. Even if information is shared appropriately to the right audience, it can stay accessible for many years and later be misused or have its meaning distorted. These long term risks are especially hard to evaluate, as normal social practice does not offer such dilemmas - oral conversation and even writings in paper are eventually lost in time. As digital storage cost continuously declines, the risk for excessively long storage of information increases. The changes one individual goes through a lifetime alone are enough for the same information to be interpreted in different ways.

Social contexts online are liquid rather than solid, boundaries are inadvertently crossed as wide audiences come together and the shared information remains indefinitely available. Technological advances enabling more data to be collected and shared only intensify this problem, making it more urgent and relevant. A social perspective should be present in all new information sharing technological developments, otherwise there is the risk of creating more problems than the ones solved.

2.2.5 Privacy in Future Scenarios

In the vision of AmI, connected devices are embedded in everyday objects, gathering data from their surroundings and enabling interaction with the environment [Punie 2003]. These devices are spread out in numerous human environments and do not require interaction to continuously provide gathered data to services. A related term that gained significant attention more recently is M2M: the technologies and business models associated with supporting communication between a plethora of connected devices as the one AmI envisions. A third *buzzword*, IoT, is many times used to describe a vision of connected objects very similar to AmI, but also used to describe the vision of ubiquitous identification and electronic representation of objects, or *things*. This second perspective is related to the use of Radio-Frequency Identification (RFID) to identify objects [L. Atzori, Iera, and Morabito 2010].

Regardless of the specific vision that is considered, the quantity of collected data by ICT systems is bound to increase dramatically in the near future, both in terms of space-time coverage and variety of data types. One of the M2M flagship scenarios is Smart Metering, which relies in collecting detailed electricity consumption data from customers in order to improve energy efficiency. However, this new type of collected information raises privacy concerns among expert groups. An European Commission working party states [Article 29 Data Protection Working Party 2013, p. 5]:

> From the detailed energy consumption data collected via the smart meters, a lot of information can be inferred regarding the consumers' use of specific goods or devices, daily routines, living arrangements, activities, lifestyles and behaviour.

These future systems have the potential for abuse by individuals, corporations and nation states, enabling surveillance and monitoring in many ways. For this reason, privacy is a key issue that has to be addressed if such systems are to produce a positive social outcome. The difficulty of this issue lies in balancing inevitable trade-off between privacy risks and service functionality [Punie 2003, p. 26].

Current privacy practices of companies in the online business only enhance privacy concerns for future scenarios. Because of the value of personal information introduced in Section 2.1.4, users' web activity is often tracked using cookies and by monitoring browser signatures [Eckersley 2010] and Internet Protocol (IP) addresses. Also, search terms are usually passed from search engines to the sites the user browses to from the search page. Finally, web activity in a site, dubbed *clickstreams*, as well as other personal information, is commonly used a revenue source for these free services. To top it off, users are usually unaware of these practices [McDonald and Cranor 2010] [Madden et al. 2013, p. 10], leaving plenty of margin for abuse. Due to the current economic incentives it is unlikely that companies will have the initiative to make their practices more privacy friendly.

Individuals are also prone to commit privacy abuses with the advancement of technology. In fact, Warren and Brandeis' privacy legal work from 120 years ago, as introduced in Section 2.1.3, was prompted by new technology that would then enable individuals to take pictures of others without needing their permission. The popularization of smart-phone cameras over the last decade similarly prompted some *shutter sound* law initiatives, mandating that smart-phones play the sound of a photographic camera shutter whenever a picture is taken. Recently, similar problems were discussed, prompted by the presentation of Google Glass [Miller 2013a; Streitfeld 2013].

The surveillance practices of US security and intelligence agencies exposed by information leaked by Edward Snowden [Greenwald 2013; Miller 2013b] also do not bode well for privacy in future scenarios. George Orwell's book *Nineteen Eighty-Four* is commonly cited [Punie 2003, p. 27] for illustrating the potential for government abuse through surveillance. In *Nineteen Eighty-Four* the *Big Brother* is an all-knowing, constantly vigilant government that regulates every aspect of one's existence. Control is exerted by targeting the private life, employing various techniques of power to eliminate any sense of privacy, namely the *telescreen*. However, in *Digital Person*, Solove proposes a different metaphor which appears to be more adequate to the current threats [Solove 2004, p. 36]. Franz Kafka's *Der Prozess* portrays an indifferent bureaucracy, where individuals don't know what is happening and have no ability to exercise meaningful control over the decisions taken about them. Transposing to present day, a large bureaucratic organization holding significant amounts of information about individuals and applying data mining techniques to evaluate, let's say, the terrorism risks an individual poses, may decide, without objective reason, that a certain individual is a threat.

As technology advances different actors get different potential for privacy abuse, which has to be appropriately mitigated if these new technologies are to be beneficial to society. Together with the advancements that enable mass collection, storage, processing and use of information, privacy mechanisms and practices have to be pushed forward.

2.3 Privacy-related Bodies of Knowledge

2.3.1 Structuring Privacy Work

As happens with the privacy concept in society, the privacy-related technical literature is quite fractured. For example, the term PETs is used to describe mostly security technologies, related to encryption. Data-centric privacy stems from a different area than the so-called PETs, and developed on its own, with seldom intersection points. Furthermore, privacy-relevant research topics related to new scenarios, such as Vehicular Ad-hoc Network (VANET) and the IoT, are typically addressed vertically, focusing on the scenario and rarely generalizing the use of studied privacy mechanisms. As the privacy issues involve more interaction with the user and less a theoretical attack model, academia provides less answers. Notable exceptions come mostly from the behavioural economics study of privacy.

In this section these multiple technical understandings of privacy are structured in one landscape, making it possible to more adequately understand the relations between different work, the impact it has in society, and where the work described in this thesis adds to the state-of-the-art. We make use of the work of Pfitzmann and Hansen which developed a consistent terminology for talking about privacy [Pfitzmann and Hansen 2010]. Although it evades a definition of privacy, it defines a number of concepts which can be used to address it. The most relevant terms are presented in advance so that they can be used to frame existing privacy work in this section, and throughout this thesis. Given an adversary that observed some events and gathered information, let us consider the following outcomes:

- anonymity - the adversary cannot distinguish the subject from other subjects within a set of all possible subjects, the anonymity set;
- unlinkability - the adversary cannot sufficiently distinguish whether two or more Items-Of-Interest (IOI) - e.g., subjects, messages, actions, . . . - are related or not.

The opposite terms are also used: linkability, naturally the opposite of unlinkability, and (re-)identification, opposite of anonymity.

2.3.2 Cryptography

The obvious, most well known, privacy-related technical bodies of knowledge are those related to cryptography, which typically focus on the security of ICT. Cryptography-based techniques generally allow building in security on top of vulnerable infrastructure. The attack model typically includes an adversary with physical access to the network, storage or computing infrastructure used by the target system. The basic purpose of the application of such techniques is preventing unauthorized reading or writing of protected data from or to a device or network message, which is an essential requirement from the privacy point of view.

Work in symmetric and public-key cryptography enabled the development of encryption protocols, namely Secure Socket Layer (SSL) and Transport Layer Security (TLS) [Hickman 1995; Freier, Karlton, and Kocher 1996; Dierks and Rescorla 2008], which allows communicating over insecure IP networks with protection against payload eavesdropping and interference. These are the most widely deployed PETs due to built-in support from major browsers and because these mechanisms are almost transparent to the user [Goldberg 2007, p. 7]. Other relevant communication PETs, for use in different contexts, include Pretty Good Privacy (PGP) [Atkins, Stallings, and Zimmermann 1996], a common solution for email encryption, and Off-The-Record communication (OTR) . OTR is an encryption solution, implemented for use in Instant Messaging (IM) , motivated by privacy flaws of the PGP approach: lack of forward-secrecy and deniability [Borisov, Goldberg, and Brewer 2004].

Although most widely deployed in communications, cryptography can also be applied in storage and computing, scenarios that became increasingly relevant with the popularization of virtualization and cloud computing. Both file system and disk level encryption are commercially available, but they are not without problems [Osvik, Shamir, and Tromer 2006; Halderman et al. 2009]. In this context the biggest promise comes from homomorphic encryption schemes. Homomorphic encryption enables performing computations on encrypted data, without the secret key, generating a result that, when decrypted, is the same as if the computations had been applied to the unencrypted data. However, due to the inherent relationship between plain and cyphertexts, homomorphic encryption is not secure enough against an attacker that employs chosen cypher-text attacks - at best it can be secure against chosen plain-text attacks [Fontaine and Galand 2007]. Some well known asymmetric encryption algorithms, such as RSA and El Gamal, have homomorphic properties allowing multiplication operations on encrypted data. Recently a breakthrough fully homomorphic encryption scheme was proposed [Gentry et al. 2009], enabling a wide range of computations on encrypted data, which has been subsequently improved [Gentry and Halevi 2011] and inspired derivate work [Brakerski and Vaikuntanathan 2011]. However, the current state of the art on homomorphic encryption still has practical application issues, especially regarding the large size of the cyphertext and computation times required [Naehrig, Lauter, and Vaikuntanathan 2011].

It is also worth mentioning two privacy goals that have originated relevant cryptography-based work: Private Information Retrieval (PIR) and Secure Multiparty Computation (SMC) . PIR work aims enabling a user to fetch some data from a server without disclosing what data he is interested in, either in an information-theoretic sense (no leaked information), or in a computational complexity sense (the adversary must solve a computationally intractable problem) [Yekhanin 2010]. A key paper in this area proposes a multi-server solution for the information-theoretic goal [Chor et al. 1998], which has been subsequently improved. For the less strict computational formulation, a single-server solution has been proposed [Kushilevitz and Ostrovsky 1997]. However, under most assumptions, using PIR solutions proposed so far is still less efficient regarding the required network traffic than the trivial solution of transfering the entire database to the client [Sion and Carbunar 2007; Olumofin and Goldberg 2012]. SMC is a more general problem as there is no server and client - all parties want to keep their inputs private while collaborating to do some computation on those inputs. Famously introduced by Yao [Yao 1982], this is tangibly described as the millionaire problem. Since then significant follow-up work has been produced [Goldreich, Micali, and Wigderson 1987; Du and Atallah 2001], sometimes dubbed garbled circuits or Secure Function Evaluation (SFE) [Bellare, Hoang, and Rogaway 2012; Naor and Nissim 2001].

The problem of securely running programs in virtual machines hosted by an untrusted provider has also been targeted over recent years [T. Garfinkel et al. 2003; Sailer, X. Zhang, et al. 2004; Sailer, Jaeger, et al. 2005; Perez, Sailer, and Doorn 2006; Feldman et al. 2010]. However, all proposed solutions are at the architectural level and would require significant changes to current systems in order to be implemented.

2.3.3 Anonymous Communication

Another class of PETs attempts to build anonymous communication systems over an unsafe communications infrastructure. The attack model is similar but, instead protecting the payload of communication, the goal is to protect the origin and destination of the payload in the unsafe network, generally accomplished by the use of some kind of overlay network. Popular work by Chaum [1981; 1988] was used to implement anonymous remailers or mixes [Goldberg, D. Wagner, and Brewer 1997, p. 7] to protect the users' real email addresses. However, these practical efforts gathered little public [Goldberg 2007, p. 4] and academic attention, and presented some vulnerabilities when studied [Serjantov, Dingledine, and Syverson 2003]. Other systems, such as onion routing [Goldschlag, M. Reed, and Syverson 1996; Goldschlag, M. Reed, and Syverson 1999], attempt to protect against IP-level traffic analysis. The second generation onion routing [Dingledine, Mathewson, and Syverson 2004], dubbed Tor, managed to get significant use [Goldberg 2007, p. 11] and some media attention [Glater 2006]. While not without problems [Bauer, Grunwald, and Sicker 2009], it enables subjects to access servers across unsafe networks while hiding which server is being accessed. A different, but related, problem is the ability to publish content for public access in an anonymous way, while maintaining content availability, even if the network over which it is being served is compromised. These technologies are specifically designed to resist censorship [Goldberg 2003]. Several such systems, which rely in distributed storage of files, have been proposed [R. Anderson 1996; Dingledine, Freedman, and Molnar 2001; Clarke et al. 2001], of which FreeNet is currently used [Goldberg 2007, p. 11] and has active developers [FreeNet Project 2013].

When the attack is done on wireless networks, additional privacy considerations are required. An adversary located close enough to a target, such that he can access to the target's radio transmissions, can easily observe low-level identifiers or determine accurate location. H. Liu et al. [2007] extensively frames and describes indoor positioning techniques, classified in triangulation, scene analysis and proximity, using on various radio-based communications, namely cellular, WiFi (802.11), Bluetooth (802.15) and RFID. A variety of fields partially addresses this issue, such as RFID and VANET privacy fields, however the approach is typically vertical, from low-level to application privacy issues. From the communications point of view, the privacy issues raised by observing 802.11 identifiers are conceptually the same as the ones raised by the abuse of RFID [Greenstein, McCoy, and Pang 2008]. Proposed techniques to mitigate this identifier observation problem typically involve hiding or rewriting [Langheinrich 2009] the identifiers. RFID tags can be killed, can answer only to authorized readers, or change their number according to some secret sequence every time it is read [S. Garfinkel, Juels, and Pappu 2005]. Regarding 802.11, frequently changing [Gruteser and Grunwald 2005] or completely removing [Greenstein, McCoy, and Pang 2008] low-level identifiers has been proposed. Preventing radio-based location beyond this would be work for an electronics or physics scholar, and falls out of scope of this thesis.

2.3.4 Data-centric Privacy

Data-centric privacy bodies of knowledge consider clearly different attack models from the previous set of fields. While previous related mostly to the gathering of data by exploiting ICT infrastructures, in data-centric scenarios the data is accessible to the adversary without an attack being required. In this field a successful attack consists in extracting information about specific subjects using data analysis techniques. Most of the times a mere re-identification, linking some database record to a subject, is sufficient for privacy to be breached. Work in this area can consider two distinct attack models that differ in the way the adversary accesses the personal data [Dwork 2006, p. 3]. In one model, data acquisition is done non-interactively: the adversary has full access to a sanitized [Chawla et al. 2005, p. 5] or anonymized dataset. The other model considers an interactive approach: there is a privacy-preserving interface between the adversary and the database, and the adversary accesses data by issuing queries [Dwork 2008, p. 3].

Because entire datasets are typically used in data mining, work done under the non-interactive model is usually called Privacy-Preserving Data Mining (PPDM). In this field, an anonymized or sanitized dataset with some set of sensitive attributes is made available, and the adversary attempts to re-identify records of the database or to discover values of sensitive attributes of subjects. In some work re-identification alone is considered to be a privacy breach [Narayanan and Shmatikov 2008], while others focus on sensitive attribute disclosure [Sweeney 2002]. Also, other work [N. Li, T. Li, and Venkatasubramanian 2007] considers that high enough probability that the sensitive attribute has a specific value is also a privacy breach. The privacy-preserving techniques studied in this field are typically sanitization algorithms which are applied to the whole dataset before it is released. Examples of operations done in these algorithms include value generalization, perturbation and suppression [Sweeney 2002; C. C. Aggarwal and Yu 2004]. Because the typical use case associated with this model is data mining, the privacy-preserving technique applied should not destroy the utility of the dataset for mining purposes.

The interactive model has been used for significantly longer than the non-interactive model, especially in the field of Statistical Disclosure Control (SDC) [Chawla et al. 2005, p. 1]. In this model the data is accessed through a mechanism which is responsible for privacy protection. This mechanism typically receives aggregate queries from a user, which can be an adversary, and returns a response based on the personal data contained in the database. The response is a perturbed version of the actual response from the database, such that the privacy is maintained. This field recently recovered interest from the scientific community [Dwork 2008] due to the work on Differential Privacy [Dwork 2006]. In Differential Privacy, Dwork formally defines a very strong privacy guarantee, which implies that it is not sufficiently distinguishable whether any given record is part of the database or not. This work places data-centric privacy in a strong mathematical foundation from which subsequent work quickly emerged over these last years [Dwork 2011].

2.3.5 Location Privacy

Location is a type of personal information especially relevant for privacy purposes. With the popularization of Global Positioning System (GPS) receivers, wireless and mobile networks, location data became widely available and enabled the creation of Location-Based Services (LBS) . This type of information is especially relevant for several reasons. First it's temporary in nature, so typically is supplied in real-time, or at least with a timestamp, to the LBS. Second, it's unique per subject and cannot vary arbitrarily - a person cannot be in two places at the same time and cannot be in opposite side of the planet in the following minute. Finally, it allows inferring a great deal about one's personal life and habits [Beresford and Stajano 2003]. Location privacy has been a popular topic in the last decade, however this work frequently considers both wireless communication privacy threats, addressed in Section 2.3.3, and pure location privacy threats [Gruteser and Grunwald 2003]. In this section the focus is on the second: privacy mechanisms that protect against adversaries with access to some location information and that intend to use temporal correlation to infer additional information about the user [Huang, Yamane, et al. 2006]. Having access to location information, an adversary may perform [Gruteser and Grunwald 2003]:

- Restricted Space Identification - link a message to a known subject because the message was sent from a geographic area to which only that subject has access to;
- Observation Identification - link two messages sent from the same location as originating from the same subject;
- Location Tracking - link a sequence of location observations to an subject by linking the subject with only one of them.

Methods to protect against the use of these correlations include spacial and temporal cloaking [Gruteser and Grunwald 2003], path confusion [Gruteser and Grunwald 2005], silent periods [Huang, Matsuura, et al. 2005; Huang, Yamane, et al. 2006] and the use of mix-zones [Beresford and Stajano 2004] - an application of Chaum's anonymity principles [Chaum 1981] in the location problem. There is also work that addresses location privacy drawing from generic data privacy techniques [M Terrovitis and N Mamoulis 2008].

2.3.6 Privacy in Distributed Systems

Despite the fields previously presented, privacy is rarely transparent to the user. Most of the times privacy mechanisms impact the use of systems, and the way a system is used carries privacy implications. A number of technologies exist to address typical privacy-related requirements, such as authentication and access control. While in monolithic systems these are trivial problems, in distributed systems complexity increases and protocols become necessary. However, as the problem-space moves further away from theory and towards the users, academia seems to have less contributions. One significant contribution is the conceptualization of privacy-enhancing IdM [Hansen et al. 2004], outlining the functions of such a system. Maybe because these problems are very functionality-related, they were promptly tackled by the industry with the development of a number of protocols and standards. One of the most well known of these protocols is OAuth, now in version 2 [Hardt 2012], which facilitates the implementation of authorization patterns by decoupling the entity issuing the authorization from the entity hosting the resource. The development of OAuth started out of an authentication project, OpenID [Recordon and D Reed 2006], and ironically hampered its adoption as OAuth started being used as a pseudo-authentication protocol [Google Inc. 2013b]. Another key standard in this area is Security Assertion Markup Language (SAML) [E Maler 2003], an extensible language capable of expressing assertions vouched by some authority, mainly used for enterprise web Single Sign-on (SSO) and web services security.

Despite these protocols enabling complex scenarios across security domains, they initially require the user to authenticate to at least one of these domains. Despite its well documented vulnerabilities, the most common authentication method remains to be password-based [Hoonakker, Bornoe, and Carayon 2009]. The implemented authentication method typically depends on the value of the service or account that the user is authenticating to [Grosse and Upadhyay 2013]. While password authentication is the most popular and cheapest method, some types of services require the use of two-factor authentication. The challenges to widely deploy these are more related to user experience and economic problems rather than technical ones.

Authentication is not only done from a client to a server, but also the other way around. Setting up an Hypertext Transfer Protocol Secure (HTTPS) connection requires the use of certificates [Cooper et al. 2008] to authenticate the remote server, so that the connection is not vulnerable to Man-in-the-Middle (MitM) attacks. Certificates are validated by the Internet's Public Key Infrastructure (PKI) , relying in root Certification Authority (CA) such as Verisign, which typically have their certificates pre-installed in web browsers. However, the current PKI is not without problems [Ellison and Schneier 2000]. A key problem is the manual and expensive nature of the verification processes that should be required before a CA issues a certificate to a website. A common approach to bypass this problem is the use of self-signed certificates for personal websites, however it's difficult for a user to verify the self-signed certificate belongs to the actual owner of the site and not to an adversary. Perspectives [Wendlandt, Andersen, and Perrig 2008] is a decentralized method to verify self-signed certificates, which assumes that attacks are either localized to a particular network scope or of limited duration, using "notary nodes" to confirm the certificate is the valid.

2.3.7 User Control of Information Flows

Beyond being able to authenticate to different systems, users need to be able to manage the access control and privacy settings of the information provided to those systems. However this is not a trivial task, and Facebook provided a number of examples of this [Bilton 2010; Helft and Wortham 2010; Bilton 2012; Sengupta 2013]. Social networks are most affected with such issues because they, like no other online community before, bring together very different users sharing information linked to their own *real-world* identities. The conflicting social queues of such diverse communities complicate the natural privacy perceptions of users [Boyd 2002], leading users to share more than they would want, typically resulting in embarrassment. Furthermore, Girão and Sarma [2009] note that current security measures that rely on user decision points interrupting the service interaction drive the user to increasingly ignore them. The key to mitigate these problems is to conveniently communicate to the users an understanding of the informations flows that can or will occur in the system, and to enable users to control what information flows where. Lederer et al. [Lederer et al. 2004] identified a number of design pitfalls that limit the user's ability to understand and act upon information flows:

- obscure the nature and extent of a system's potential for information disclosure;

- conceal the actual information flow - what information is disclosed to whom;
- excessive privacy configuration overwhelms users - privacy should be part of the normal use of a system;
- lack of an obvious, coarse-grained, privacy control;
- inhibit users from applying established social privacy practices in a technology context.

An example of bad communication regarding the potential information flows in systems is the complexity of web site privacy policies. McDonald and Cranor attempted to quantify the cost of reading the site's privacy policies and the result greatly outweighed the value of the targeted advertising market that personal information feeds [McDonald and Cranor 2008]. Furthermore, the actual understanding of users regarding what sites do with their personal information is far from reality [McDonald and Cranor 2010]. A proposed solution for this problem was Platform for Privacy Preferences (P3P) [Cranor, Langheinrich, et al. 2002] which would allow matching the machine-readable privacy preferences of sites with the browser-configured privacy preferences of users. However, P3P was not widely adopted because of its complexity and low perceived added value. A very simple alternative approach was suggested [Raskin 2010; Raskin and Ranganathan 2010]: using symbols to transmit privacy policy meaning, much like Creative Commons. This work was improved and documented within Mozilla [Mozilla 2011], but shows no record of application. Another lightweight alternative, Do Not Track (DNT) [Mayer, Narayanan, and Stamm 2011], consisting of simply including an Hypertext Transfer Protocol (HTTP) header in requests indicating to the web server that he is not allowed to collect, retain, or use any data related to that request and associated response, is gaining momentum [Soghoian 2011a]. However, none of theses solutions provide privacy by themselves, they mere improve privacy-related communication between web users and service providers. They require to be supported by legislation and that enforcement is conducted by regulatory authorities.

2.3.8 User Behaviour Regarding Privacy

Even if users understand the impact of their privacy actions, their choice is seldom predictable. There are several examples where public misconduct or sharing embarrassing information happens with the purpose of getting others attention. Privacy economics tries to understand and quantify the costs and benefits of sharing or hiding personal information [Acquisti 2009]. Applying economics to users' privacy choices revealed what is known as the privacy paradox [Smith, Dinev, and H. Xu 2011, p. 12]: users state they are concerned about privacy, but act in apparent contradiction with this [Acquisti 2004; Acquisti and Grossklags 2005]. There are a number of hypotheses to explain this phenomenon, namely the existence of a bias towards immediate benefits comparing to long-term risks [Acquisti 2004], as well as the *control paradox*: control over the publication private information decreases individuals' privacy concerns and increases their willingness to publish [Brandimarte, Acquisti, and Loewenstein 2012]. The behaviour of users when disclosing their personal information to companies is object of analysis not only in privacy and security scientific communities [Grossklags and Acquisti 2007] but also in marketing and accounting [Pavlou 2011]. Economics can not only be used to study user behaviour but also to analyse the theoretical incentives of actors in distributed privacy systems, using a game theoretical approach [Acquisti 2003; Domingo-Ferrer 2011].

2.4 Conclusions

Internet users consume online targeted advertising based on browsing information transparently collected about them, post personal information, pictures and videos of them to social networking sites, and enable information to be gathered and used by *Apps* in their smart-phones. The business model of the Web 2.0, offering users free services in exchange for their data, is a major area of privacy-related discussion. Behavioural economists attempt to understand the apparently miopic behaviour of these users, while technologists attempt to influence enterprises to declare their data handling processes in a machine-readable way. On the enterprises side, security techniques are employed in order to safeguard the wealth of collected data from internal misuse and external attackers.

While these techniques can safeguard enterprise aggregated data from attackers, they offer no protection against legal entities. The current surveillance practices of US governmental intelligence and security agencies confirmed some of the fears of the *cypherpunk* movement. Privacy techniques that guarantee privacy without requiring any legal safeguards have to be applied by users themselves. However, these same techniques that can protect individual liberties from overzealous security agencies and the threat of a surveillance state, obviously also work against other legal methods, facilitating the conduction of illegal activities online.

Existing privacy-related work is provided by different technical disciplines, addressing different levels of privacy problems, and in some cases different problems altogether. However, all technical areas can contribute a little to each of the different privacy problems. In order to reach conclusions about the applicability and relevance of privacy techniques a classification exercise needs to be conducted, especially relevant for the privacy approaches of new use cases. The vertical style of privacy analysis abundant in the fields of VANET, IoT and context awareness needs to be decomposed and framed within existing focused work. In turn, focused work cannot be used independently of each other because the models that allow them to be comprehensive and effective solutions also restrict them to a set of assumptions and a problem level. Privacy has to be addressed holistically, at all levels, from the computing and networking infrastructure to the behavioural incentives of actors in the system, otherwise the techniques applied at one level can be attacked at another.

Chapter Three

Communications Perspective

This chapter presents a range of work which can contribute for controlling information flows in distributed systems, a fundamental building block for privacy in a networked world. The vision of an Identity Layer for a social-pervasive scenario is put forward, developed under the Societies project.

3.1 Introduction

3.1.1 Networked World

Almost 40% of the world's population uses the Internet and, considering developed countries alone, the figure rises to 74.8% [Teltscher et al. 2013]. The services provided through it are part of the everyday life of millions of people. However, the use of Internet services leads to constant distribution of information about oneself. Simple web searching and browsing provides valuable interests information that is turned into revenue through targeted advertising, as introduced in Section 2.1.4. A search query, meant to find some information online, as a post in a social networking site, meant to communicate something with a group of friends, disclose information about users to the providers of those services. Furthermore, mechanisms exist to enable one service provider to access information stored in another provider, further increasing the data distribution chain. Finally, individual service providers rarely clarify how the data gathered this way is used, and whether it is further distributed.

The very use of the Internet, disregarding the actions of web service providers, can enable an attacker with privileged access to the network to monitor one's communications. While encryption is known to be an effective protection to communication content against most adversaries, as introduced in Section 2.3.2, it does not hide the fact that two parties were communicating. This information alone, disregarding the communicated data, can be very revealing, and thus a threat to privacy.

At the centre of personal data communication issues is the field of IdM, addressing the control and management of the linkage between different identifiers and attribute values, as introduced in Section 2.3.1. It has implications both in the network perspective of privacy, where the linkability of different network-level identifiers is addressed, as well as in the distributed systems perspective, as it can be used to enable attribute value access authorizations and such functionality.

3.1.2 Chapter Outline

In this Chapter the main issues regarding personal data communication control are addressed. Network-level privacy issues are over-viewed, the concept of identity in a networked world is outlined and the mechanisms that allow users to control what data is communicated about them, and how it is communicated, are discussed. Section 3.2 starts by discussing the benefits and limitations of encryption and existing techniques to overcome privacy threats based on traffic analysis. Section 3.3 addresses IdM issues, focusing on the management of multiple identities online in a distributed environment, and describes the IdM approach taken in the Societies project. Section 3.4 focuses existing solutions for controlling information flows between different systems, both *a priori* and *a posteriori* of the moment of disclosure.

3.2 Communications Security and Anonymity

3.2.1 Encryption's Achilles Heel: Key Authentication

Encryption plays a central role in communications security and privacy, as described in Section 2.3.2. It enables data, or payloads, to be securely delivered across insecure networks, where attackers that can eavesdrop at all points of the network. This assumes that the sender and the recipient of the payload had previously agreed on an encryption method and keying material. Encryption can be symmetric, where the same key has to be known to both communicating parties, or can be based in public-key cryptography where each party has a key pair, one public that everyone can access and one private that must be kept secret from other parties. Besides encryption, public key cryptography can be used for key exchange for symmetric encryption (e.g. in TLS [Dierks and Rescorla 2008, p. 91]) and, less relevantly from a privacy point of view, for digital signatures (e.g. in PGP [Atkins, Stallings, and Zimmermann 1996, p. 3]). Public-key cryptography is based in the intractability of some mathematical problem: the private key is almost impossible to derive from the public key. The most common mathematical problem used currently for public-key cryptography is integer factorization (e.g. RSA [Rivest, Shamir, and Adleman 1978]). However, due to existing sub-exponential time algorithms so solve integer factorization [Koblitz, Menezes, and Vanstone 2000, p. 174], elliptic curve cryptography [Koblitz 1987] was proposed, using an alternative mathematical foundation. Encryption protocols, namely SSL and TLS [Hickman 1995; Freier, Karlton, and Kocher 1996; Dierks and Rescorla 2008], are the most widely deployed PETs due to built-in support from major browsers and being transparent to use [Goldberg 2007, p. 7]. These typically rely in public-key cryptography to authenticate the server, so that the protocol is not vulnerable to MitM.

However, public-key cryptography is only as strong as the means to assert that a certain public key is in fact controlled by a certain entity or person, i.e. the authentication of that public key. In the Internet, web servers authenticate to browsers using a certificate [Cooper et al. 2008] that is signed by a CA - this is the Internet's PKI. However, as discussed in Section 2.3.6, the existing PKI has been criticized for many years [Ellison and Schneier 2000]: the whole is only as strong as it's weakest link, which seem to be the CAs. Recent attacks to two such authorities, Comodo and DigiNotar, enabled hackers to issue certificates signed by those CAs enabling them to pose as high-profile websites [Leavitt 2011].

PGP [Atkins, Stallings, and Zimmermann 1996], the popular email encryption solution that also uses public-key encryption, solves the authenticity of public keys problem with the *web of trust*. Instead of using a centralized trust model such as the current web PKI, the model is distributed. It relies in individual users signing each other's public keys as if asserting that the key belongs to that person. When communication is required between two users that don't have prior contact, they can choose to trust the remotely provided public key based on the *introducers* that have asserted the authenticity of the key belonging to that user. As public keys are signed by more users, trust webs emerge around communities [Abdul-Rahman 1997].

The centralized PKI solution relies too much in the security practices and ability of CAs, the web of trust places this burden in the activity and security practices of users. The centralized option is more practical as it does not require users to manage trust, but a compromised CA has significantly more severe security problems than a compromised PGP private key. A pragmatic compromise between accessibility and security was found for Secure Shell (SSH) authentication [Ylonen and Lonvick 2006], known as *leap-of-faith* authentication [Arkko and Nikander 2004]. On first use, users have to decide whether an unknown key is valid or not, based on the key's fingerprint that can be confirmed by other means. If the key is considered valid than it is cached and used to authenticate subsequent communications with that remote host.

A recently proposed alternative to traditional PKI, dubbed Perspectives [Wendlandt, Andersen, and Perrig 2008], builds upon leap-of-faith authentication. It describes a decentralized method to verify self-signed certificates, which assumes that MitM attacks are either localized to a particular network scope or of limited duration. The validity of keys is measured by its association to a specific server over some period of time. Perspectives uses an infrastructure of *notary nodes* to provide geographical and temporal resistance to MitM attacks. Based on this work, a Firefox add-on dubbed Convergence was released [Thoughtcrime Labs 2011]. While the attack model considered here is not as strong as the omnipresent attacker, typically used in network security, the work remains interesting as the restrictions placed on the attacker's ability are very reasonable. As Abraham Lincoln put it [Wendlandt, Andersen, and Perrig 2008], "you can fool all the people some of the time, and some of the people all the time, but you cannot fool all the people all the time."

3.2.2 Communications Anonymity

Even if data payloads are kept secret with encryption, access to the unencrypted network identifiers that enable communications, such as IP and MAC addresses, is sufficient for threatening privacy in several ways [Matos 2012, Sec. 3.4.2]. A common requirement is to be able to hide the origin and destination of communications done on an insecure network. Chaum [1981] first tackled this problem, describing a system of anonymous remailers or mixes to protect the users' real email addresses. Based on this work, a number of types of mixes were implemented and deployed [Goldberg, D. Wagner, and Brewer 1997, p. 7]. One such implementation, known as *Mixmaster remailers*, includes countermeasures against a number of passive eavesdropping attacks, such as size and time correlation attacks. However, it shows vulnerabilities to active attacks involving blocking most messages arriving to the mix or flooding the mix with attacker-generated messages [Serjantov, Dingledine, and Syverson 2003].

Onion routing [Goldschlag, M. Reed, and Syverson 1996; Goldschlag, M. Reed, and Syverson 1999], bring these principles to the IP level. The second generation onion routing [Dingledine, Mathewson, and Syverson 2004], dubbed Tor, is currently a popular solution for anonymity in internet communications, used by criminals [Roy 2013] and whistle-blowers [Greenberg 2013] alike. It does not waive the use of standard encryption and other privacy techniques, but is considered a resilient technology for preventing IP-level traffic analysis [Tor Project 2013]. Tor is a *peer-to-peer* protocol which relies on the dimension of the network to anonymize communications. When a Tor node starts it chooses 3 nodes to create a *circuit* that will be used for the anonymization. IP packets are encapsulated in 3 encryption layers and sent to the *circuit*, coming out in their original form at the exit of the third node. Each node of the circuit only knows its predecessor and successor, not being able to determine both the origin and destination of the actual message.

Obviously, it is not without problems. A simple denial of service can be done by blocking access to the centralized directory servers [D. Anderson 2012]. Also there is a class of attacks that relies in the *performance over anonymity* orientation of Tor [Bauer, McCoy, et al. 2007; Bauer, Grunwald, and Sicker 2009]. In order to provide low latency in routing, enabling the support interactive applications, Tor does not re-order, batch or generate noise traffic, as email mixes do. Furthermore, the anonymizing routers forming the Tor path are selected based on their perceived bandwidth capacities, skewing router selection toward routers with higher bandwidths. Adversaries can leverage on this property by providing adversary-controlled routers with high bandwidth to the Tor network. If an adversary controls the first and last routers of a path it can then apply timing attacks correlating origin and destination.

3.3 Identity Management

3.3.1 Foundations and Definitions

Philosophically speaking, *identity* distinguishes one subject from another. It is also a social construct of how a person conceives themselves and by extension how others see that person [Mead 1934]. Pfitzmann and Hansen [2010] formally define Identity as *the negation of anonymity and the negation of unlinkability*, based on the concepts of anonymity and unlinkability introduced in Section 2.3.1. In other words, identity is any subset of attribute values of an individual person which sufficiently identifies this individual person within any set of persons. So in this context there is no such thing as *the identity*, but several of them. A *partial identity* is a linkable 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. While one identity sufficiently identifies an individual person (without limitation to particular sets of subjects), a partial identity may not do so. A partial digital identity is the digital representation of a partial identity.

Having defined identity, let us set the foundations for dealing with a special type of attributes: *identifiers*. Identifiers are attribute values that are unique (at least with a very high probability) within any set of subjects, negating of anonymity, and that are relatively stable across time and context, providing some linkability. *Pseudonyms* are a type of identifiers which typically are less stable and hold less side-information than normal identifiers, such as one's real name and e-mail address. Based on a name or e-mail address it's possible to use the data from the string itself to derive more information without access to any additional attributes - e.g. it's possible to infer information from the domain of an e-mail address of from one's family name. With pseudonyms little side-information is included in the identifier string, or none at all in case it is a random string. Regarding their stability across time and context, an identifier such as name or e-mail is typically used for a long time (years) in a wide variety of contexts - personal, professional, behaving as a customer and as a provider. In contrast, pseudonyms are typically - but not necessarily - used only in specific contexts or for a limited amount of time.

Pfitzmann and Hansen [2010] distinguished types of pseudonyms based in their usage:

- person pseudonym: substitute for the subject's name which may be used in many different contexts - e.g., a number of an identity card, the social security number, DNA sequence, a nickname, the pseudonym of an actor, or a mobile phone number;
- role pseudonym: used only in specific roles - e.g., a customer pseudonym, a personal e-mail address or professional e-mail address;
- relationship pseudonym: for each communication partner a different pseudonym is used - e.g., distinct nicknames for each communication partner;

- role-relationship pseudonym: for each role and for each communication partner, a different pseudonym is used;
- transaction pseudonym: for each transaction a different pseudonym, unlinkable to any other pseudonym and at least initially unlinkable to any other IOI, is used - e.g., randomly generated transaction numbers for online-banking.

The subject which the pseudonym refers to is the holder of the pseudonym. When the subject is a partial digital identity, the identifier is usually a pseudonym [Hansen et al. 2004] due to similarly having a limited scope.

3.3.2 Privacy-enhancing Identity Management

IdM is managing various partial identities, denoted by pseudonyms, of an individual person, i.e., administration of identity attributes including the development and choice of the partial identity and pseudonym to be (re-)used in a specific context or role. Then, privacy-enhancing IdM is done in a way such that, given the restrictions of a set of applications, unlinkability (as seen by an attacker) is sufficiently preserved between the partial identities and corresponding pseudonyms of an individual person [Pfitzmann and Hansen 2010, p. 34]. The re-use of a pseudonym allows continuity to be supported in a specific context or role, by enabling linkability with former or future IOI. For IdM to be privacy-preserving this linkability should only be possible if such is desired by the user [Hansen et al. 2004]. Furthermore, outside of the context or role in which a specific partial digital identity is used, that partial identity should be as identical as possible to a non-existing identity.

A system that addresses these issues needs to enable role taking and making for all applications, managing what pseudonyms are used and what attributes are released within each communication or transaction. This management has to be aware that secrecy is not always the goal. The uncontrolled creation and acceptance of pseudonyms can lead to problems such as Sybil attacks [Douceur 2002]. To address these problems, Martucci et al. describe a pseudonym-based trust-enabled identity scheme for the Internet of Services [Martucci, Ries, and Mühlhäuser 2011] that only needs to rely in a Trusted Third-Party (TTP) in the bootstrap and pseudonym issuing phases. The trust approach is distributed, enabling users to freely decide whether to divulge service provider recommendations or not, enabling privacy on that specific type of data. The TTP in charge of issuing and managing pseudonyms is usually denoted Identity Provider (IdP) .

Trust is not only important regarding the identifier, but also regarding the attributes associated to it. Some use cases require that users use attribute values belonging to one identity context in a different one. Through the use of cryptographic techniques it becomes possible to prove something regarding an attribute value without disclosing the associated pseudonym by using some credential issued by a TTP [Hansen et al. 2004]. In many IdM approaches the IdP accumulates both and the responsibility of issuing pseudonyms and attribute credentials. Contrary to the rule, work done in the SWIFT European project decouples these two functions, introducing the Attribute Provider to deal with the second one [Barisch et al. 2010].

The use of a TTP is a common mechanism to balance privacy and trust requirements. However, according to the multilateral security principle [Rannenberg 1993; Rannenberg 2000], all parties should be regarded as potential attackers. Different parties may have different and sometimes conflicting security goals, and the level of trusted placed on other parties should be minimized. Centralized IdM solutions that rely on an all-knowing IdP are therefore in disagreement with this principle [Hansen et al. 2004]. The level of trust placed in each TTP should be architecturally minimized by distributing them across different parties, making misuse less attractive and limiting the harm that can be done [Rannenberg 2000].

IdM is a complex topic which has implications in different areas. One of the broadest approaches is probably the work in the Daidalos projects resulted in the concept of Virtual Identity, a cross-layer partial identity of an entity [Girão, Sarma, and Aguiar 2006]. The entity can be a user, a group of users, or service and network providers. The proposed architecture in Daidalos2 preserves linkability between different Virtual Identities of the same entity, both from the service and network provider point of view. The described federation model enables data associated with a Virtual Identities to be interoperable across different administrative domains by semantically mapping it [Aguiar et al. 2006].

Changes in identity systems are also associated to changes in communications paradigms. For example, Sarma and Girão envision the Future Internet of Things as an *Identinet* where each endpoint, independently of being a person, a service or software, is represented by an identity. This Identinet provides some device independence as what matters is the entity that the device is operating on behalf of. Also, by employing identity management techniques, it has the potential to enable enhanced security and privacy for users [Girão and Sarma 2009].

3.3.3 Identity in the Web

When addressed for the Web, identity problems mostly focus on authentication and attribute access mechanisms. The term *walled gardens* is widely used to describe the web of sites that came to be with the Web 2.0 model. Each of these sites holds his own silo of user attributes, along with application data, requiring that users go through a sign-up process every time they start using a new web application and through a login process each time they use it. In 2005 the first signs of change to this scenario emerged. First, Hardt coined the term Identity 2.0 in his OSCON keynote presentation as the shift from these data silos to a user-centric IdM paradigm, where the user presents one of his certifier-issued identities to access whatever resource or application he wants. A few months later OpenID [Recordon and D Reed 2006], the first authentication delegation protocol for the web, was released. The protocol allows users to authenticate with the same credentials, typically username and password, to a large number of web applications. These application providers, called relying parties in OpenID terminology, don't have access to the credentials, instead trusting an IdP to assert that the user is who he says he is - the holder of a specific identifier.

However, OpenID was not without problems. It was designed having in mind simplicity and scalability, in order to be suitable for the web, and chooses not to address some complex problems such as trust and IdP to relying party (or service provider) unlinkability [Eve Maler and Drummond Reed 2008]. Also, an empirical study [S.-T. Sun et al. 2011] identified a number of shortcomings, most related to the authentication user interfaces: many users did not understand how to use the system nor its benefits, and some were tricked into phishing attacks. Furthermore, a significant ammount of users expressed concern in using OpenID to authenticate both to high-value and untrustworthy relying parties. Finally, security problems have been identified due to the lack of integrity protection in requests [Sovis, Kohlar, and Schwenk 2010].

OpenID was a landmark development in identity for the web, despite its limited success, as the user relies solely on his unmodified browser for using the scheme. A different class of IdM solutions for the web encompasses the use of enhanced browsers or clients, as the one proposed by S.-T. Sun et al. [2011]. These include, most notably but with modest adoption, the now defunct Microsoft InfoCard and Mozilla Persona, built on the BrowserID protocol [Mozilla Developer Network 2012]. A third type of solutions requires the existence of a personal server in order to enable user-centric authentication, or to provide generic access to all kinds of user attributes. WebID [Story et al. 2009; Inkster, Story, and Harbulot 2014] is a protocol that re-uses widely deployed TLS and a personal web server in order to enable browser authentication, by proving that the user of the browser controls a certain URL. More generically, Personal Data Services, such as the Higgins project [Eclipse Foundation 2009], enable service providers to request attributes from a user-controlled server. However, due to the requirement of having a personal trusted server, the adoption of these solutions is extremely impractical given the current over-centralized state of the web.

The adoption of any web authentication delegation mechanism requires web service providers to delegate part of the user information they would normally have direct access to. Being in possession of personal information is the value that major web companies turn into revenue, as referred in Section 2.1.4. Furthermore being the holder of the user identification services became a strategic objective for these companies. In the past couple of years Facebook enabled third parties to delegate authentication to Facebook, first for web sites and afterwards for mobile applications in iOS and Android operating systems. Google, on the other hand, merged the YouTube user accounts to Google Accounts, and requires that Android users are logged in with their Google Account to be able to use key functionality like the Android application store *Google Play*. Recently Google became an accredited IdP for some US government applications [Schmidt 2011]. The strategy of these major IdP clearly involves increasing the number of users and relying service providers as much as possible, contributing to changing the Web 2.0 walled gardens into an iron curtain.

3.3.4 Federation and Single Sign-On

In the enterprise world, where solutions tend to be more comprehensive and planned, rather than organic and flexible like in the Web, the problem of using only one set of credentials to authenticate in many systems is referred to as Single Sign-on (SSO). A subsequent step to SSO is the use of attributes from one system in another and vice versa, sometimes across different security domains. For that reason it is necessary to establish a mapping between the attribute names in the different domains - in one system the user's name attribute may be called *realName* and in the other there may be two attributes, *givenName* and *familyName*. When two different domains can interoperate in terms of user authentication and data they are said to be *federated*.

One of the most relevant developments in IdM for the enterprise was the Liberty Alliance Identity Federation Framework (ID-FF), a set of protocols that collectively provide a solution for identity federation management, cross-domain authentication and session management. This specification was contributed to Organization for the Advancement of Structured Information Standards (OASIS) , forming the foundation for SAML 2.0, which is currently used in the widely deployed Shibboleth SSO solution and adopted by the OASIS Web Services Security Technical Committee for the WS-Security specification. SAML is an Extensible Markup Language (XML) based language to communicate authentication, authorization and attribute information in a secure and trusted way. The specified protocols associated to it enable web SSO, among other secure information exchanges.

3.3.5 Towards an Identity Layer: SOCIETIES Communication Framework

While the use of unlinked pseudonyms to separate different contexts has been well studied, their adoption has been rather limited, as mentioned in Section 2.3.2. Deployed IdM solutions are limited to enable SSO and trusted attribute communication. Reasons for this might include the cross-layer issues that a pseudonym solution has to deal with, as well as the need to address this problem in a cross-cutting manner [Hansen et al. 2004; Matos, Girão, et al. 2007; Matos, Sargento, and Aguiar 2007], instead of as an integration problem.

Societies was an European project with a consortium of 16 partners, executed from October 2010 to March 2014. It was the largest integrated project out of the fifth call for project submissions for FP7, and was rated *Excelent* at the final review. The project aimed to bring together social and pervasive computing into one integrating platform. The proliferation of user owned networked devices has untapped potential that can be capitalized by allowing device capabilities to be offered on the network as services, information and resources. These devices would together form a Cooperative Smart Space (CSS), a digital representation of a user or organisation, enabling the sharing of user-owned services, information and resources. CSSs constitute the users' bridge between the physical world and the digital social communities the user is a part of. A community is a collection of CSSs and/or supporting infrastructure services, who wish to collaborate for mutual agreed purpose for which the community formed. The community's digital representation is called a Community Interaction Space (CIS), through which users can access and make available services, information and resources [Doolin et al. 2012].

As part of the work developed for this thesis, in Societies an identity layer mechanism was devised and a prototype implemented [SOCIETIES 2011]. This identity layer can best be described as a pseudonym-enabled federated identity layer, drawing from the Identinet vision [Girão and Sarma 2009], enabling users to have more privacy without loss of functionality. The service providers may still access to the user's information, necessary to fulfil some function, but their ability to build a general purpose user profile with it would be severely hampered. Furthermore neither service providers nor users would be restricted to a specific IdP. TTP must exist in order to enable liability and assurance scenarios and to prevent Sybil attacks [Douceur 2002] but, in agreement with multilateral security principles, these entities should have minimal responsibilities. This is achieved with an open federation of IdP, where different IdPs can be used to interact with the same service providers, and where users can freely change IdPs.

The described open federation is slightly different from the concept of federation usually considered in Web and enterprise SSO. While this one mainly refers to the semantic interoperability of user attributes between domains, the open federation we

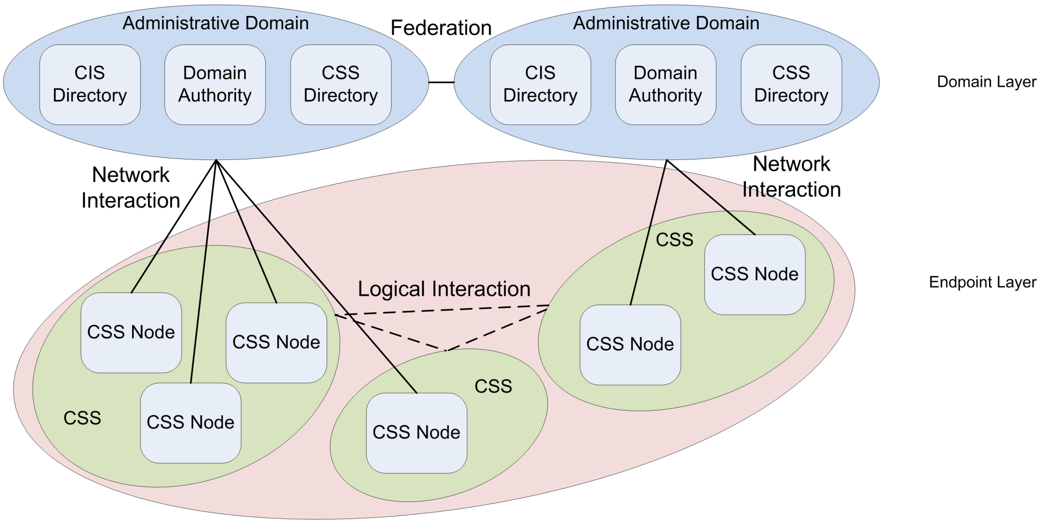

Figure 3.1: Open Identity Layer Architecture

consider is more about enabling open communication between domains independently of the attributes being passed around. In the Societies architecture the attributes are provided and consumed by entities and services, not the domain administering entity, so the semantic interoperability responsibility lies with them. The domains just need to provide the infrastructure for these different services and entities to communicate securely and privately.

In an open federation scenario is useful to consider the term *identity domain*. An identity domain is an identifier namespace administered by one IdP. Since identifiers are unique in their domain, an identifier and domain pair absolutely identifies a partial digital identity. Subjects can authenticate with the IdP, named Domain Authority (DA) in Societies, w.r.t. identifiers that belong to the domain it administers. In Figure 3.1, the two-layer IdM architecture is depicted, showing how different endpoints in different domains can interact. The Domain layer provides the trusted identity, discovery and communication services, while service providers and users interact with each other, communicating data linked to different identifiers, on the Endpoint layer.

CSS is a distributed construct that represents a single user in the digital world. In order to create a CSS account the user must choose a DA, based on his perceived trust for that entity. The DA is the entity responsible for authenticating the user devices associated to a CSS, and for making the devices, dubbed *CSS Nodes*, belonging to the same CSS to be known to each other. It must provide functions to support the creation of new CSS accounts, which may imply some offline verification process. It must also provide support for the association of new CSS Nodes, normally done by proof of ownership of existing Nodes.

Besides providing authentication and pseudonym issuing services, the DA also performs other privacy and identity related functions that need to be somewhat centralised. First it behaves as an anonymizing communication proxy between different entities, preventing lower-layer identifiers to be used to link messages. Unless a CSS already has a trusted communication context established, communication should go through the DA. This approach requires the DA to be a message router, making it also suitable to perform the identity-based routing that is necessary for having identity-addressed network endpoints, as idealized by Girão and Sarma [Girão and Sarma 2009]. Furthermore, the DA also enables entity search and service discovery.

While the DA is a centralised component from the point of view of the endpoints, it is a distributed if we consider that they are automatically connected with other DAs in an open federation, enabling communication, identity-based routing and entity search across domains. This realises the concept of an identity layer as an open federation decoupled from specific applications. Also it enables users to freely choose their IdP based on their opinion or identity purpose, not having to choose the one most of their friends use, or that their favourite applications support. This would enhance competition between IdP in their core service value: privacy policies, security practices, credibility, and so on.

In an open federation any entity can host a domain, enabling individual users to run their own DA. However, the fewer users a domain has, the easier it is to identify them since the domain of an identity is publicly known. When users choose a DA they are effectively *hiding in the crowd* of users in that domain.

Pseudonym management is done on the user devices, on behalf of the user, with support from the DA for pseudonym issuing. Three types of pseudonyms are defined:

- Public pseudonym: human-readable identifying strings, meant to make the user globally contactable, managed explicitly by the user and not to be used as a service consumer;
- Facet pseudonym: optionally human-readable string, meant to identify the user in the continuous use of a service or communication with another party;
- Transient pseudonyms: random strings meant to make the user contactable within the scope of a transaction or in the establishment of a trust relation that leads to the issuing of a facet pseudonym.

Public pseudonyms are the ones meant to make the user contactable, similarly to email addresses. These are managed explicitly by the user, and typically are used in different social circles and communities. Users explicitly create and manage the public data associated with them to make themselves as searchable as they wish. Facet pseudonyms are used to contact one or a few related services or users. They are like a chat room nickname or a web application username: they enable temporal linkability in a restricted context. Transient pseudonyms are mostly used when the user is accessing a stateless service, or a service where only limited temporal linkability is required. Its use typically spans over a few transactions. Transient pseudonyms are also used to contact a remote entity before a trust relation is established with that entity, which may lead to the issuing of a facet pseudonym.

The implementation effort of this vision was much larger than the effort available in Societies for this purpose, so only a partial implementation was provided to the project. The implementation, dubbed Communication Framework, relied in an XMPP infrastructure to provide identity-based routing, abstracting the network as much as possible - components only need to know what is the identifier of the remote entity [Gonçalves and Gomes 2014]. XMPP is an Internet Engineering Task Force (IETF) protocol and its open extensions, XMPP Extension Protocol (XEP) , are supervised by the XMPP Standards Foundation. It is a bi-directional XML messaging protocol, originally aimed for IM, built directly on top of Transmission Control Protocol (TCP) , which can provide an extensible messaging infrastructure, with built-in federation mechanism, supporting endpoint authentication, resolution and presence, message routing, asynchronous messaging and some degree of reliability. In recent years XMPP has been adapted for other applications than IM, such as VoIP [Ludwig et al. 2009] and microblogging [Saint-Andre et al. 2012].

Furthermore, transparent data object serialization was provided so that components could remotely communicate data objects abstracting how data is represented on the wire. The implementation was done for Java 1.6, using OSGi and Spring Dynamic Modules integrated in the Virgo platform [Eclipse 2011], and for Android 4.0. Open source XMPP libraries were used in the implementations: Smack [Ignite Realtime 2002b] and Whack [Ignite Realtime 2002c]. For the transparent object serialization, after unsatisfactory results with JAXB [Java.net 2003], SimpleXML [Gallagher 2006] was adopted due to its Android compatibility. While the resulting prototype was not enough to demonstrate the potential of an pseudonym-enabled identity layer, it was enough to show its advantage from an architectural point of view [Gonçalves and Gomes 2014]. Furthermore, Societies project partners used the code to develop their research [Vardjan and Porekar 2013; Kalatzis et al. 2013] and the platform was tested in user trials [Doolin 2013]. The source code is available at Github [SOCIETIES 2011].

3.3.6 The Importance of Data in Pseudonym Management

Freely providing the same attribute values under different pseudonyms can enable an attacker to link these pseudonyms. For this reason, with the ability to issue and communicate using pseudonyms, function that allows monitoring their association and vulnerability to linkability has to be considered. Pseudonym generation and re-use should take in account this function that analyses which pseudonyms are more suitable for interacting with some service or entity. While the final decision should rest with the user, the system should provide the necessary tools for the user to make an informed choice regarding his pseudonym use [Hansen et al. 2004].

This function, dubbed *Identity Selection* in the Societies project, supports user decisions by estimating the knowledge that observers have of the user's pseudonyms. It keeps track of interactions and disclosed information for each partial digital identity, as it happens in associated research [Vardjan and Porekar 2013]. Because of all the data the function has access to, it must run in a user-controlled device on behalf of him. The most appropriate pseudonym is typically the one that minimises partial digital identity linking risk while satisfying the requirements of data disclosure from the remote entity. Users will typically re-use existing pseudonyms when interacting with the same remote entities or releasing the same attributes [Hansen et al. 2004]. If the re-use of the natural pseudonym for the given context is too risky the user should be properly informed in order to take a decision. Some pseudonyms may be intentionally heavily re-used, e.g. if the user wants to play the role of a well-known service provider. The system should give the user the best conditions possible in order for users to take informed decisions, but must not take invisible decisions on his behalf [Hansen et al. 2004]. Protecting privacy is a lot about having a system behaving the way users expect it to.

Besides considering attribute disclosure history between entities there is also the need to consider the nature of the disclosed information, namely uniqueness and stability. One possibility to do so is by taking an information theoretical approach. Shannon's entropy [1948] can help us estimate how unique a piece of information is, how much information it actually carries - e.g. if a user discloses his current city this gives us more information about him than if he discloses his current country. Each disclosed value about the user may be translated in a quantifiable amount of anonymity loss [Eckersley 2010]. Since we are dealing with multiple and most likely dependent data items, in which the total anonymity loss is less than the sum of the individual values for data disclosure, joint entropy would be a candidate information theoretical foundation for these estimations. Specific attacks on unlinkability provided by privacy-enhancing IdM using re-identification techniques have been identified by Claußet al. [Clauβ, Kesdogan, and Kölsch 2005]. Possible countermeasures have to re-identification done at the data level have to come from the PPDM field, as introduced in Section 2.3.4 and discussed in Chapter 5.

3.4 Data Flow Control

3.4.1 Access Control and Authorization

Adequately controlling data flows between systems is among the most fundamental privacy requirements. Permission is usually required when a remote system is contacted in order to provide some data stored there. The requesting party needs authorization to access that data or the data server needs to perform an access control check in order to determine whether to deny or allow the request. Authorization and access control are different points of view to address the problem of protecting resource access in distributed systems: authorization is seen mostly from the requesting party point of view, leading to solutions that promote easy data access, while access control is seen from the data server point of view, tending to privilege restraint.

Much like authentication, only recently distributed resource protection started being seen as cross-cutting function with re-usable logic and patterns. It has historically been looked at as a functional requirement of a system, and implementations were usually case-specific. It was in order to improve interoperability in the area that Extensible Access Control Markup Language (XACML) was developed. Version 3, super-seeding the previous version from 2005, was recently released by OASIS, a standards organization. XACML specifies an XML-based language for specifying resource access policies in a standard way, designed primarily for use in an enterprise scenarios, typically with Web Services, but flexible enough to be applied to different types of resources. A typical access control scenario involves three entities - a subject, a resource and an action - which relate as follows: the subject requests performing an action on a resource. The access decision, resulting from the access control policy and request, may depend solely on these entities or also on attributes such as time of the day. Based on this model, XACML defines an architecture comprising of 4 components:

- Policy Enforcement Point (PEP) - entity that gets the request that needs to go through an access control check;
- Policy Decision Point (PDP) - central point of the architecture, receives XACML requests from the PEP and generates a decision, and subsequent response based on the existing policies;
- Policy Administration Point (PAP) - supplies access control policies to the PDP;
- Policy Information Point (PIP) - supplies relevant information to the PDP;

The main components are the PEP and the PDP. It is between them that the access control requests and responses are exchanged. An XACML request represents a question: whether a given subject can do a given action to a resource. The PDP calculates the decision based on the policies it has defined. XACML defines an XML format for the policies. A policy refers to a target and contains a number of rules. Based on the request information, the PDP navigates the policies looking for a match in the target. When it does, it returns the associated access decision.

As introduced in Section 2.3.6, OAuth is an IETF protocol which decouples authorization roles, allowing clients to access remote resources more easily. The first version [Hammer-Lahav 2010] was developed out of need during the OpenID implementation for the Twitter external Application Programing Interface (API) as there was no authorization delegation functionality defined. It enables accessing protected resources without requiring authentication credentials. OAuth2 [Hardt 2012], the second version of the protocol, has faced difficulties in its standardization process with the withdrawal of lead author and editor Eran Hammer due to disagreements over the direction of the work. Hammer disagreed with the excessive enterprise orientation of OAuth2, resulting in an overly complex specification, less interoperable and useful than its predecessor [Hammer 2012]. OAuth defines four roles:

- resource owner - entity capable of granting access to a protected resource, typically the end-user;
- resource server - server hosting the protected resources;
- client - application making protected resource requests on behalf of the resource owner and with its authorization;
- authorization server - server issuing access tokens to the client, after successfully authenticating the resource owner and obtaining authorization.

Put as simply as possible, an authorization grant is given by the resource owner so that a client can access some protected resource. In the presence of the authorization grant, the authorization server issues an access token to the client, enabling it to fetch the protected resource from the resource server.

The use of OAuth grew quickly with the popularization of web APIs, becoming the de-facto standard for lightweight and flexible authorization delegation. Precipitated by the success of OAuth, a new version of the OpenID protocol was developed, OpenID Connect, relying heavily in OAuth2, an authorization protocol, to delegate authentication. The underlying idea is that an authentication relying party requests authorization to access the user's identifier, as if it was any other attribute, from an OpenID Connect provider.

While OAuth focus on the practical problems of authorization delegation, XACML aims at flexible access control policy definition. They cover different aspects of the distributed resource protection problem and thus is possible to use them together. However, having been developed with different spirits and purposes, concrete use cases will typically ask for the use of either one or the other.

3.4.2 Privacy Policies

Privacy policies define the company policies regarding data collected throughout the use of a service. They describe what data is gathered and what happens to it: for what purposes is used, for how long is kept and whether is shared with third parties. While resource protection deals with permissions to access data, possibly preventing a service provider from gathering said data, the privacy policy applies when either the service provider can directly gather some data or has the authorization to retrieve it from another party. Currently service providers mostly provide privacy policies as legal safeguards, having no restrictions as to their format, length readability or content

[McDonald and Cranor 2008]. Most of these policies are written in *legalese* and typically thousands of words long - Facebook's Privacy Policy increased from 1004 words in 2005 to 5830 in 2010 [Bilton 2010].

Lorrie F. Cranor, a reference author in the field, co-authored a study which does an economic analysis on privacy policies [McDonald and Cranor 2008], estimating the overall cost to read them and comparing it to the value of the online advertising market - the market where these service providers typically operate. The opportunity cost of the time required to skim once a year through the privacy policies of visited sites for all Americans far outweighs the value of the online advertising market in the US. This almost anecdotal study is a complement to another studies indicating that most users do not read privacy policies [Privacy Leadership Initiative 2001], and that a majority of users has the mistaken belief that the mere presence of a privacy policy means that a corporation will not share their data [Turow 2003]. As referred in Section 2.2.5, web service providers use a number of techniques to gather browsing information from users even if the information is not directly conveyed, namely cookies, clickstreams, and tracking techniques exploiting the uniqueness of browser signatures [Eckersley 2010] and IP addresses. Also, search terms are usually passed from search engines to the sites the user browses to from the search page, using the HTTP *referrer* header.

As mentioned in Section 2.3.7, Cranor had been the lead author of the P3P specification [Cranor, Langheinrich, et al. 2002] a few years before, which defines a machine-readable language for privacy policies for web sites. The foundations for P3P are economic: to change privacy from a *credence* good, that cannot be evaluated by the consumer, to a *search* good, which can be evaluated before consumption. It's the same principle as for the nutrition labels that are mandatory in case of food products. This change would contribute to the privacy practices of service providers to be easily taken in account when choosing one, enabling providers to compete for better practices [McDonald and Cranor 2008].

P3P defines an XML-based machine-readable representation of a privacy policy, designed to describe web service provider privacy practices, namely the types of data or data elements collected and how these will be used. The P3P XML schemas define over 30 types of elements for representing the policy and over 150 user data types that can be considered. For each data practice which can be identified, web service providers shall identify:

- the type of data that is collected, based on the specification's data types;
- the purpose of the data collection, which may include:
  - complete the current activity for which the data was provided;
  - for the technical support and administration of the Web site;
  - for enhancing, evaluating, or otherwise review the site, service, product, or market;
  - tailor or modify content or design of the site where the information is used only for a single visit;
  - create or build a record tied to a pseudonymous identifier, used to determine the habits, interests, or other characteristics of individuals for purpose of research, analysis and reporting;
  - create or build a record tied to a pseudonymous identifier, used to determine the habits, interests, or other characteristics of individuals to make a decision that directly affects that individual;

  - determine the habits, interests, or other characteristics of individuals and combine it with identified data for the purpose of research, analysis and reporting;
  - determine the habits, interests, or other characteristics of individuals and combine it with identified data to make a decision that directly affects that individual;
  - contact the individual, through a communications channel other than voice telephone, for the promotion of a product or service;
  - for the purpose of preserving social history as governed by an existing law or policy
  - contact the individual via a voice telephone call for promotion of a product or service;
- which legal entities will be able to access the data, namely:
  - the web service provider itself and/or entities acting as our agents or entities for whom we are acting as an agent;
  - entities performing delivery services possibly following different data practices;
  - entities following our practices;
  - entities following different practices;
  - unrelated third parties;
  - public fora such as bulletin boards or public directories;
- and its data retention policy, determining that information is:
  - destroyed following the online interaction with the site and must not be logged, archived, or otherwise stored;
  - retained to meet the stated purpose, being discarded at the earliest time possible.
  - retained to meet a stated purpose, but the retention period is longer because of a legal requirement or liability;
  - retained under a service provider's stated business practices;
  - retained for an indeterminate period of time.

The P3P specification also defines how the machine-readable policy can be located in a web site, enabling P3P-enabled browsers to transparently fetch it. The browser would fetch the policy and process it against the user's privacy preferences. In case the web site's policy is in agreement with the user's preferences browsing would proceed normally, otherwise the user would have some interaction with the browser, e.g. via pop-ups, requesting acceptance of the policy point which is in disagreement with the user preferences. However, a negative, privacy preserving, decision from the user would lead to an interrupted browsing experience.

The initiative faced significant criticism, especially from privacy advocates, claiming that P3P fails to establish privacy standards, lacks enforcement, is hard to implement and it's adoption will face a *chicken and egg* problem [Electronic Privacy Information Center 2000]. To respond to such criticism, Cranor et al. evaluated the adoption of P3P four years after its promotion to W3C standard [Cranor, Egelman, et al. 2008]. A list of popular search terms was used to create 1160203 search hits from AOL, Google, and Yahoo!. Of these results, 113880 were for sites that had P3P policies available, showing an approximate adoption rate of 10%. The adoption is strongest for e-commerce and US government websites. When only e-commerce related search terms are used the adoption rate rises to 21%, and among the search hits which have *.gov* as top-level domain this value rises to 39%. The E-Government Act, which mandates that government agencies published machine-readable privacy policies on their websites, is highlighted as a particular influence in the adoption of P3P. The study also evaluates the accuracy of the supplied P3P policies and found large numbers of syntactic errors and discrepancies between P3P policies and their natural language counterparts. Despite acknowledging that better tools are required for managing machine-readable and natural language privacy policies, the authors assert the errors were not critical and the discrepancies did not impact significantly the evaluation of a policy.

In the web browsers side, only Microsoft Internet Explorer implements the standard, while Chrome, Firefox and Safari have simple cookie-related privacy settings. These typically involve the deletion of cookies after the browser is turned off, blocking cookies entirely or only from third parties. In 2010, Cranor and other Carnegie Mellon University researchers studied the misuse of P3P's compact policies by websites [Leon et al. 2010]. A total of 33139 websites were studied and syntax errors or semantic conflicts were detected in 11176 of them (34%). Almost all these errors (98%) resulted in cookies remaining unblocked by Internet Explorer under default privacy settings. The authors also found thousands of sites using identical invalid compact policies that had been recommended as workarounds for Internet Explorer's P3P implementation. The Internet Explorer Team reported that Google similarly uses an invalid P3P policy format [Hachamovitch 2012], in an announcement prompted by a different technical issue - Google's circumvention of Safari's default cookie-related privacy settings [Mayer 2012].

Maier [2010], the president of TRUSTe, the leading privacy seal provider, explains this as a rational developer response to the failure of P3P:

> When a lack of mainstream P3P adoption resulted, some developers created a way to remove a perceived consumer annoyance in IE browsers.

TRUSTe is a private company that awards online privacy seals to web sites, a privacy practice endorsed by the FTC. TRUSTe requires companies to follow some basic privacy standards and to document their practices. TRUSTe also investigates consumer allegations that licensees are not abiding by their policies. However, this approach has been criticized [McDonald and Cranor 2010] and one study showed that companies with TRUSTe seals typically offer less privacy-protective policies than those without TRUSTe seals [Jensen and Potts 2003]. The disagreements between TRUSTe and the Carnegie Mellon University research group led by Cranor are obvious.

Maier further criticises the complexity of P3P by referencing a learned lessons paper by someone involved in its standardization process [Schwartz 2009]. In this paper Schwartz argues that as future PETs are developed they should be kept simple - there should be no more than four privacy options and the default setting should be set higher than average practices today. Furthermore he argues the previously mentioned *chicken and egg* problem doesn't exist because the clear way is working with the browser vendors to implement the support for the PETs, as shown by P3P. Finally, even if PETs become an alternative to legislation, the development of PETs will not be well-served by parties that engage in it in order to influence the regulatory debate.

3.4.3 Simpler Web Privacy

Simpler alternatives to P3P have been recently suggested, as introduced in Section 2.3.7. One such alternative [Raskin 2010; Raskin and Ranganathan 2010] relies in the standardization of privacy options and their visual representation. Inspired by the Creative Commons approach, symbols that transmit privacy policy meaning were drafted, hoping to communicate privacy policy meaning to users quickly and effectively. While the work was improved within Mozilla [Mozilla 2011], it shows no record of application.

A lightweight alternative that recently gained momentum and backing from the FTC [Soghoian 2011a], is DNT [Mayer, Narayanan, and Stamm 2011]. It's technically implemented by simply including an HTTP header in requests indicating to the web server that he is not allowed to collect, retain, or use any data related to that request and associated response. Browsers should include a simple configuration for the inclusion of the header. The specification has been implemented in all major browsers and by a number of advertising networks [Mayer and Narayanan 2013]. However, similarly to P3P, DNT merely improves privacy-related communication between web users and service providers. The enforcement of *no tracking* must be conducted by regulatory authorities, such as the FTC, and supported by legislation. Criticisms to the approach come unexpectedly also from the legal side, saying such initiatives deviate the legal discourse from making fundamental trade-off decision about what are and aren't acceptable web tracking practices, focusing on providing users with legal protection for a choice they aren't prepared to make [Tene and Polenetsky 2012, p. 357].

Another privacy-protection mechanism which is widely implemented in major browsers is the *private browsing* mode. Unlike DNT, this mechanism is purely technological: it limits local browsing-related information, such as browsing history and cookies. Keeping no browsing history records enables protection against local attackers, that may want to check or retrieve the user's browsing history having access to his device. Volatile cookies, that are deleted when the user closes the private browsing window, protects against cookie-based linking of browsing activity, commonly performed by targeted advertising networks. However, private browsing functionality is not the same across all browsers, and even if the cookies are temporary other mechanisms are available in private mode that can be used by a remote attacker to link private browsing sessions with non-private ones [G. Aggarwal et al. 2010]. Also, concern has been raised regarding the false privacy expectations that this mechanism may give users, possibly encouraging them in engaging risky online behaviour [Soghoian 2011b].

A proposed solution to harmonize privacy and behavioural advertising requirements is Adnostic [Toubiana et al. 2010], a browser extension that runs the behavioural targeting algorithm on behalf of the ad network. The ad to be displayed is determined by user's browser, using browsing history information, and inserted in the page. Information about the user's preferences would only be released as he clicks ads to browse the advertised product or service.

3.5 Conclusions

Privacy issues in communications can be seen from diverse perspectives, involving different fields in each perspective. The objective is often to prevent disclosure (i.e. collection) or dissemination (i.e. distribution) of data. Such preventive techniques focus on *a* *priori* privacy protection. Preventing disclosure of data is usually done to protect from attackers in the network, as discussed in Section 3.2. One party want to communicate some data to another party, and the goal is to protect the data and sometimes also the fact that the two parties communicated. Preventing the dissemination of data, on the other hand, is a distributed systems problem. It assumes that some remote system is rightly storing some personal data from an individual, and aims controlling the access to that data by other systems. Solutions for this type of problem were presented in Section 3.4.1.

In many cases, however, technically preventing the disclosure or dissemination of data is not a goal because the data is required by some service provider to fulfil some service. In these cases mixed solutions with technological and regulatory components emerge in an attempt to enforce *a posteriori* privacy protection, such as P3P and DNT. The generic goal of these solutions is to give users tools to choose and communicate whether they consent to some web service provider data capture and handling practices. However, as user behaviour is difficult to understand (see Section 2.3.8) and privacy trade-offs difficult to communicate, the effectiveness of these approaches has been frequently questioned.

Privacy-enhancing IdM is a field with the potential to balance privacy and functionality, as described in Section 3.3.2. The generic nature that enables such flexibility, involving many *a priori* privacy protection perspectives, is also the reason why it can be attacked at every level. From the network side, identifiers can be used to attack the unlinkability of different pseudonyms belonging to the same individual [Hansen et al. 2004]. From the data side, a set of attribute values can sufficiently isolate a number of pseudonyms so that the same goal is achieved [Clauβ, Kesdogan, and Kölsch 2005].

A previously proposed network privacy architecture, that assumes IdM as part of the application layer, defines out a vertical, cross-layer approach [Matos 2012]. Alternatively, an Identity Layer approach was explored in this thesis, as part of the work in contributed to the SOCIETIES project. An Identity Layer tightly integrated with encryption in order to minimize key authentication problems would effectively separate the two attack levels - network and data - allowing them to be addressed in more restricted attack models. Because cookies are the technical support of current identities in the web, an Identity Layer would obsolete them providing means of storing data on the user-side that cannot be used to excessively link his activities.

Furthermore, the benefits of an *Identinet* and of the distributed characteristics of a service-oriented ecosystem built over such an Identity Layer are explored in [Gonçalves and Gomes 2014]. Such system would differ from traditional service-oriented architectures because it attempts to counter the current centralization *status quo* of the web in favour of a service ecosystem composed by user-hosted peers that can behave at the same time as service consumers and providers. Finally, information flow control mechanisms built on top of an Identity Layer facilitate client-side monitoring and auditing, as shown by Vardjan and Porekar [Vardjan and Porekar 2013].

Chapter Four

Context-awareness and Ambient Intelligence

Context-aware systems are presented, covering enabled scenarios, existing architectural approaches and privacy work specific for this area. The shortcomings of current solutions, namely their unsuitability for real-time adaptation, are analysed. This chapter contains contributions to the state-of-the-art, published in three conference papers and a journal, regarding context-awareness scenarios, an event-based approach to context management, and a low-latency access control system addressing the key context-specific privacy issue while complying with the real-time nature of the context delivery process.

4.1 Introduction

4.1.1 Context-awareness and Future Visions

The vision of AmI, which oriented European ICT research for the last decade [Punie 2003], is close to become possible. Users will daily interact with dozens of connected devices, many times not explicitly as devices are embedded in human environments. These devices may gather data from their surroundings and enable actuation on the physical environment. The communication challenges for the realization of this vision are being addressed under the M2M umbrella, namely wireless and wired communication to both low-powered and unconstrained devices, remote device management and data communication [Wu et al. 2011]. Work in this area has attracted interest from the Telecommunications industry as providing a connectivity service to these devices may be a business model for the future. This *connected objects* vision is also frequently referred to as the IoT, despite this being considered an *Internet*-oriented vision. A more unique perspective of IoT, under a *Things*-oriented vision, is the use of RFID tags and readers in order to identify and electronically track objects and goods [L. Atzori, Iera, and Morabito 2010], enabling a wide range of new use cases.

The goals of context-awareness are included in the AmI vision: contextual information relevant for an application or service is gathered and used for adaptation and improved user interaction. While AmI doesn't restrict itself to context-awareness, it makes extensive use of the reactivity that context-awareness enables. Similarly to what happens in M2M and IoT, information is primarily gathered via connected objects capable of sensing the physical world around them. However, the service use cases related to these two paradigms aren't the typical sensing-actuating scenarios of context-awareness. The emphasis is on data gathering and mining in order to enable tailored value-added services. Where context-awareness commonly requires *real-time* updates for its adaptation scenarios, in most M2M and IoT scenarios only *up-to-date* information is required, where a delay of some minutes is acceptable.

4.1.2 Towards Ambient Intelligence

The term *context-awareness* was introduced more than a decade ago. Much has been written and done related to this area since then, contributing to a state-of-the-art that appears to be sufficient for the realization the scenarios that were laid out, some of them included in the AmI vision. In a widespread adoption scenario different systems would use context information acquired from the same sources, delivered by means of a context delivery system, promoting reuse and transmission optimization of context information. However the context-aware applications that managed to get some commercial success are vertical, relying either on user devices or environment sensors to gather their own context information and use it for a specific application. The most relevant are probably LBS such as Google Latitude, Foursquare and Gowalla (before being acquired by Facebook), which gathered significant user bases in just a few years. However, these services are typically vertical and social-oriented: a user manually shares at what venue or public place he is at the moment, based on a list of existing venues in the area, crowdsourced from users of the service, and on the user's location. Users can usually also search for nearby venues (restaurants, pubs, . . .). The only context-aware adaptation that takes place in these services is assisting the user finding venues based on his current location. The de-verticalization of context information gathering and consumption is a key step towards the realization of the AmI vision, as having hundreds of vertical services consuming the same types of context information directly from the sensors would be unmanageable and inefficient.

Another key requirement, even further away from being achieved, is reactivity. The success of HTTP and of the client-server model is heavily influencing the approaches taken for future data services. As example, a key proposed M2M standard [European Telecommunications Standards Institute 2011] perpetuates the request-response model, ideal for scenarios where centralized servers held all the required data. In order to deliver information from sensors to applications in a timely manner, the distributed interaction model must be primarily event-oriented instead.

Finally, privacy aspects are essential to the social acceptance of these future scenarios [Punie 2003]. In a world where large quantities of information are made available by a variety of devices, and that part of that information is used to provide, adapt and improve services, it becomes key to align the amount of information required with the amount of information disclosed. Technical mechanisms that minimize the quantity, precision or freshness of communicated information, given the requirements of active services, are especially relevant this scenario. Regarding non-reactive use cases using historical context information, the privacy protection problem is similar to the one in current database scenarios, addressable by methods introduced in Section 2.3.4 and discussed in Chapter 5.

4.1.3 Chapter Outline

More formal context-awareness definitions are presented in Section 4.2, as well as common requirements and scenarios, including two scenarios developed within the scope of this thesis. In Section 4.3, after analysing existing architectural solutions, architectural instantiations of context-aware services, and an event-based context-management platform, are presented. In Section 4.4 the state of the art in context privacy is analysed. Drawing from access and disclosure control techniques from Section 3.4 the event-based architecture is extended to support real-time complex context disclosure control mechanisms. This enhancement is presented in Section 4.4, with the other context privacy work, and thoroughly discussed in Section 4.5.

4.2 Foundations of Context-Awareness

4.2.1 Definition

The most often used definition of context is given by Abowd et al. [1999]. These authors refer to context as

> any information that can be used to characterize the situation of an entity (a person, place, or object) that is considered relevant to the interaction between a user and an application, including the user and applications themselves.

According to this description, if we disregard application domains, context information can be practically any information as long as it is related to some entity. The generality of this definition is pointed out by Winograd [2001] despite the value brought by the emphasis on the relationship of that information with an entity - person, place or thing.

The classification of specific context information is then a frequent topic in literature, probably because of this definition problem. Again, Dey and Abowd define four primary types of context information: identity, activity, time, and location. These primary types of context information answer the questions of “who?”, “what?”, “when?”, and “where?”, and they can be used to get other sources of context information. Other popular classification method is the distinction of different context dimensions. Prekop and Burnett [2003] and Gustavsen [2002] call these dimensions external and internal, and Hofer et al. [2003] refer to it as physical and logical context. The external/physical dimension refers to context that can be measured by hardware sensors (i.e. location, light, sound, movement, touch, temperature or air pressure) whereas the internal/logical dimension is mostly specified by the user or captured by monitoring and inferring user interactions (i.e. the user’s goals, tasks, work context, business processes, the user’s emotional state).

Frequently associated with the context information definition discourse are the scenarios enabled by context-awareness. There are three categories of features that context-aware applications can exhibit [Abowd et al. 1999]:

- presentation of current context information to a user;
- automatic execution or adaptation of a service; and
- storing interrelated context information for posterior processing.

While the first and third feature categories can easily be identified in M2M and IoT scenarios, the human-interactive nature of context awareness is unique to the AmI vision. This is also the one that has the stricter set of requirements, as will be discussed in the next Section.

4.2.2 Capabilities and Requirements

In order to drive context-awareness closer to reality, some authors proposed a set of functionalities and capabilities that should be present in such a system. Pascoe [1998] identified four core capabilities in order to support context-awareness in wearable systems in a generic way:

- contextual sensing: simple detection of environmental changes using sensors;
- contextual adaptation: application behaviour change given these changes;
- contextual resource discovery: discovery and exploitation of context resources; and
- contextual augmentation: associating digital data with a particular context.

While it is clear that these capabilities are somewhat generic, Pascoe’s validation and examples are restricted to location information, the type of information used in his validation scenario. Furthermore, the scenario application allowed users to visualize location and attach that information to notes taken by the user. The described system is not distributed and there is no reactive or adaptive feature in the application.

Dey, Abowd, and Salber [2001], based on their more generic context-awareness vision introduced in previous work [Abowd et al. 1999], propose a wider set of requirements for a context-enabling framework:

- Separation of Concerns: separation of how context is acquired from how it is used (i.e. one sensor can provide context to a number of different applications and applications can easily get context information from different sensors);
- Context Interpretation: high-level socially relevant context is inferred from low-level physical context information (e.g. a meeting can be detected based on co-location, sound levels and schedules);

- Transparent and Distributed Communications: because sensors may be physically distributed, a network and a global time synchronization mechanism are required, so that context is communicated in a comparable and combinable way;
- Constant Availability of Context Acquisition: because context acquiring components run independently of applications, and their information may be needed at any moment, these components must be always running;
- Context Storage and History: context acquiring components should maintain a history of all obtained context in order for prediction and tailoring functionality to be implemented;
- Resource Discovery: in order for an application to communicate with a context acquiring component, it must know what kind of information the component can provide, where it is located and how to communicate with it (protocol, language and mechanisms to use).

These authors recognise the need for transparent communications and time synchronization mechanism, but say nothing about timely delivery. A limit on context delivery latency is a key hidden requirement for adaptation scenarios, as described in previous Sections. The maximum delivery latency depends on the type and precision of the transported context information: more precise and dynamic context information has tighter latency constraints. As example, the user location expressed in terms of city doesn't need to be updated in the exact second that the user leaves the city limits, while the precise indoor location used for smart-building adaptation, such as lighting and door lock controls, does. Assuming that the adaptation scenarios are for improving human interaction with systems, the latency limits are bound by human perception and reaction times. From the field of cognitive psychology, the value of 190 milliseconds for human visual reaction time [Kosinski 2008] is considered as a context delivery latency reference throughout the work presented in this Chapter.

4.2.3 Scenarios and Business Value

From all the scenarios possible with context-awareness, the ones explored in work related to this thesis are taken as examples of the provided functionality and business potential. These scenarios were studied and developed by building upon context management work done in the C-CAST project, and were published in conferences [Simões et al. 2009; Gonçalves, Delahaye, and Lamorte 2010].

The Context-aware Triggering System [Simões et al. 2009] has the ability to trigger a reaction to a specific occurrence or a set of events. This is a key functionality in context-aware systems, due to its reactive nature, and can be considered both as a standalone application or as a building-block for other services. Two use cases are presented, respectively one for each of the two approaches: a geo-fence messaging application and a targeted advertisement trigger service. The geo-fence messaging application considers the contacts the user has, as well as their demographics, presence and location, in order to trigger automatic messages which can promote social encounter or as heads up for arrival to a meeting or gathering. The business value of this application is especially directed to Telecommunication companies as the automatic messages would be charged to the user as a regular text message or data in their mobile phone.

The second use case is a targeted advertising scenario where advertising companies can send targeted campaigns towards their customers or even aiming at new clients that are willing to receive commercials in exchange for some other benefits (discounts or gifts). The use case focuses on users in proximity of a number of sell-points or shops. The information about the available goods and promotions is available. Although the advertisement is triggered by location, the advertisement selection also take the goods and promotions information as well as the user preferences into consideration. Let different shops have their triggers and respective content set-up under approximately the same location, an airport. Several context information types associated with the defined triggers are pro-actively being monitored by the context triggering application. At some point in time, a user triggers (due to location) several different ads which are then ranked in order to decide which ad to deliver. Advertisement is the main source of revenue for web companies, so the value potential of this service is very appealing.

Context-aware Content Rating [Gonçalves, Delahaye, and Lamorte 2010] is the intelligent context-aware ranking of multimedia content, both professional and user-generated. Techniques typically used in recommender systems rely in the manual rating of content by users in order to recommend content. However, regardless if the recommendation techniques are content-based (i.e. recommends based on content similarity) or collaboration-based (i.e. recommends based on user similarity), they are vulnerable to the *new user/item problem*: until the new item is rated by a substantial number of users, or the new user rated a substantial number of items, the recommender system would not be able to produce meaningful recommendations [Adomavicius and Tuzhilin 2005]. Furthermore these recommender systems create a static user profile that does not consider the specific context the user is in. Context-aware Content Rating enables rating of content suitability based on metadata and context-information alone. Instead of using content ratings, service providers can rate content based on:

- location - the user is to get more content related to where he is located;
- presence and calendar - if the user is busy or has free time he may be interest to get only essential information or time-sink content;
- proximity - if the user is co-located to another users then he may be interested in similar content those users are consuming;
- preferences - if the user is interested in politics, sports, finance or other category he should get more content about that.

One use case is tourist cultural content delivery: as a tourist goes around town in the bus, historic site presentation videos are played in order, based on his location and profile information. In between the historical videos, restaurant or hotel advertisements are played, based on location and on the advertisement contracts.

While these scenarios are promising in terms of user experience and business value, the privacy problem that context awareness might cause are a key obstacle to their commercial implementation. In Section 4.3 the architectural foundations for implementing these scenarios are discussed, and in Section 4.4 privacy aspects of context management systems are addressed.

4.3 Architectures for Context-Awareness

4.3.1 Context Management State-of-the-Art

From these requirements it is defined a conceptual context-enabling framework that is composed of five building blocks: widgets, interpreters, aggregators, services and discoverers [Dey, Abowd, and Salber 2001]. The applications make use of these to implement context-aware behaviour relying on a comprehensive set of functionalities.

Context widgets acquire context information. Interpreters transform and raise the level of abstraction of context information, possibly by combining multiple pieces of context. Aggregators gather context information related to an entity for easy access by applications. Services execute behaviours on the environment using acquired context - they are actuator abstractions. Finally, discoverers allow applications to determine the capabilities of the environment and to take advantage of them.

This widget model is one of the models analysed by Winograd [2001], in addition to his blackboard model and to a networked services model described by Hong and Landay [2001]. This networked services model aims to decrease the coupling towards the context acquisition components. The context acquisition components act as servers and can be accessed at will, independent of location, by dynamic discovery or configuration. The blackboard model is a flexible and loose-coupled data-centric model where information sources can be added transparently, but not the most optimal because all context messages are generic and every communication requires two hops. H. Chen, Finin, and Joshi [2003] and H. Chen, Finin, and Joshi [2004] defined a Context Broker Architecture (CoBrA): an agent based architecture for supporting context-aware systems using a central agent called Context Broker (CxB) . This architecture, similarly to Winograd's blackboard, defines a generic context model. Additionally, it is responsible for acquiring context information for resource-limited devices, reason about context information, detect and resolve inconsistent context information, and protect user privacy by enforcing policies that the users have defined.

Some EU-funded projects that addressed context management also opted for a broker-based architecture, namely MobiLife [Floréen et al. 2005] and C-CAST [Zafar et al. 2009]. The main difference of both these approaches when compared to Winograd's blackboard model and Chen's CoBrA is the main method of obtaining context information: MobiLife and C-CAST define it as a query initiated by the peers, instead of a notification from the CxB when context changes occur. Similarly to Chen's CoBrA, these Context Management Architecture (CxMA) define a generic context model and decouple context acquisition from consumption, but delegate reasoning to external components. Furthermore, both projects define the Context Provider (CxP) and Context Consumer (CxC) architectural entities as part of addressing separation of concerns - the CxP feeds context information into the system, and the CxC fetches it.

Another EU-funded project, MUSIC, developed a middleware platform [Paspallis et al. 2008] which exposes an API to supply, query for and be notified about context information. Also under this project a new context model was specified [Reichle, M. Wagner, Khan, Geihs, Lorenzo, et al. 2008], as well as a Context Query Language (CQL) [Reichle, M. Wagner, Khan, Geihs, Valla, et al. 2008] which enables filtering and aggregation of results while querying for some context information. This language was later adapted for use in the C-CAST CxB architecture. Another example of middleware solution is Gaia [Román et al. 2002]. Gaia makes use of five core services: Event Manager Service, Context Service, Presence Service, Space Repository Service and Context File System. The Event Manager decouples context suppliers and consumers, allowing them to communicate via channels where message persistence is guaranteed. The Context Service provides the system with tools to handle the chosen generic context model. The Presence Service maintains information about the existing entities in the environment. The Space Repository Service allows the system to know about existing computing and output resources and their properties. Finally, the Context File System provides storage that builds virtual directory structures based on context, allowing files to be accessed easily based on some context information. Another example is the SOCAM middleware [Gu, Pung, and D. Q. Zhang 2004] that makes use of an ontology based context model and defines three basic components, Context Providers, Context Interpreters and Service Locating Service, in order to support context-aware mobile services. The Context Interpreters that take in low level context to provide higher level context, using reasoning and a context knowledge base, and are integrated in the platform similarly to the approach adopted in C-CAST, by using the typical CxC and CxP interfaces. The Service Locating Service provides discovery functionality for the existing resources.

These CxMA target the problem of enabling context-awareness functionalities in a reusable and convenient way for different scenarios and applications. However, in order for the proposed solution to be easily adopted, the architecture should enable context and service providers controlled by different entities and belonging to different security domains to establish trust relationships and to interoperate. These requirements are generally captured by the notion of the federation mechanisms which should be considered in a CxMA.

Another issue with the analysed CxMA is the reaction time of the resulting context-aware systems. The most interesting types of context information to use are usually quite dynamic and variable in time (ex. location, temperature, ambient noise levels, . . .). For these to be used in AmI adaptation scenarios, context-aware services need to be notified of relevant context changes in near real-time. As mentioned in Section 4.2.2, the human notion of real-time can be drawn from the field of cognitive psychology. For a CxMA to enable services to receive context changes in under 190ms it clearly cannot rely in polling mechanisms for fetching content. A CxMA supporting adaptation scenarios must have an event-oriented mechanism that as primary method of context dissemination.

Furthermore, the benefits of a generic context representation adopted by some of the proposed solutions are not clear. Introducing a new generic context representation language increases the complexity of the solution, without reaping a clear benefit. Existing extensible data formats exist that have diverse characteristics required by the different solutions. These should be used in order to maximize interoperability. Finally, the discovery mechanisms proposed are typically complex, and sometimes coupled with the actual context information querying process. For greater flexibility, context discovery and delivery should be decoupled.

4.3.2 Context-awareness in Service-oriented Systems

The earliest contributions to the state of the art from the work presented in this thesis are related to the development of the C-CAST context-awareness architecture [Zafar et al. 2009]. Based on this work two architectural work-tracks emerged, introducing context-awareness pre-existing architectures [Simões et al. 2009; Gonçalves, Delahaye, and Lamorte 2010] in order to implement the scenarios described in Section 4.2.3. In order to do this, a service-oriented approach was taken, integrating the context management platform in more complex systems composed of *service enablers*. Each of these enablers brings a different, self-contained set of functionality to the system.

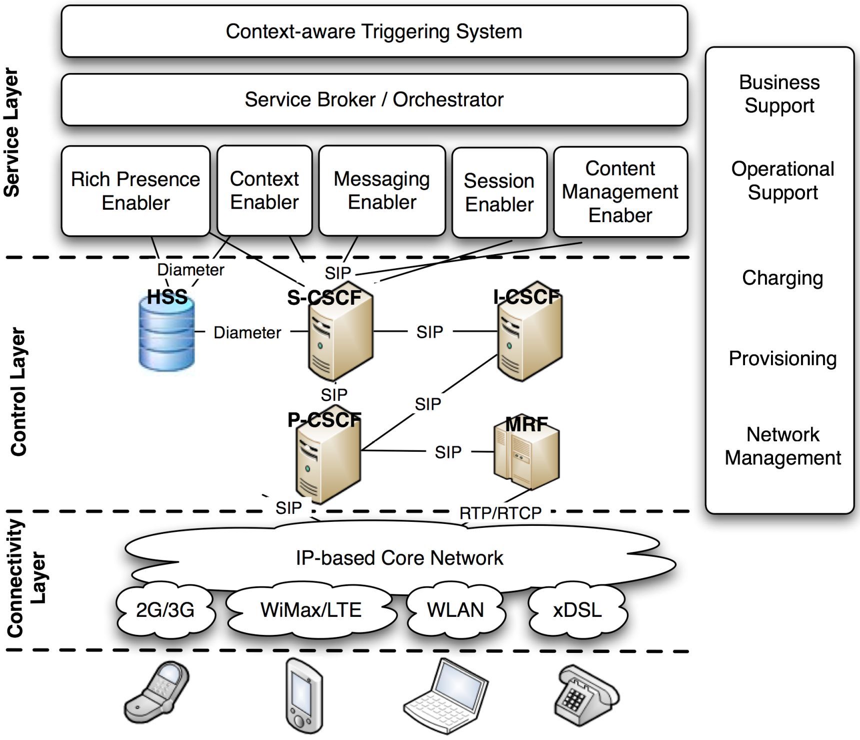

Figure 4.1: Overview of the Context-aware Triggering System Architecture

The first context-awareness integration resulted in the development of the Context-aware Triggering System, using IP Multimedia Subsystem (IMS) [Simões et al. 2009]. This system relies in five service enablers in order to deliver rich context-based triggering functionality, as shown in Figure 4.1: Rich Presence Enabler, Messaging Enabler, Session Management Enabler, Content Management Enabler and Context Enabler. The Context Enabler is the C-CAST Context Management platform used as a building block to deliver reactive Telecommunications services. The service enablers communicate using a service integration layer, dubbed Service Broker / Orchestrator, providing discovery and configurable service-oriented communication between the enablers. Below the enablers an IMS platform is used for executing the trigger actions, independently if they involve simple messaging or a multimedia session.

The second context-awareness instantiation in a service-oriented system was a multimedia content rating system [Gonçalves, Delahaye, and Lamorte 2010], aimed at recommending multimedia content, both professional and user-generated, relying on contextual information instead of manual ratings. Four enablers are required for this system, depicted in Figure 4.2. Similarly to what happened in the Triggering System, Content Management, Context Management, and Content Delivery functions are provided by enablers. The content rating is provided by the Content Selection Enabler which takes enriched content meta-data from an advanced Context Management Enabler and compares it against the context information based on configuration provided by the specific content service.

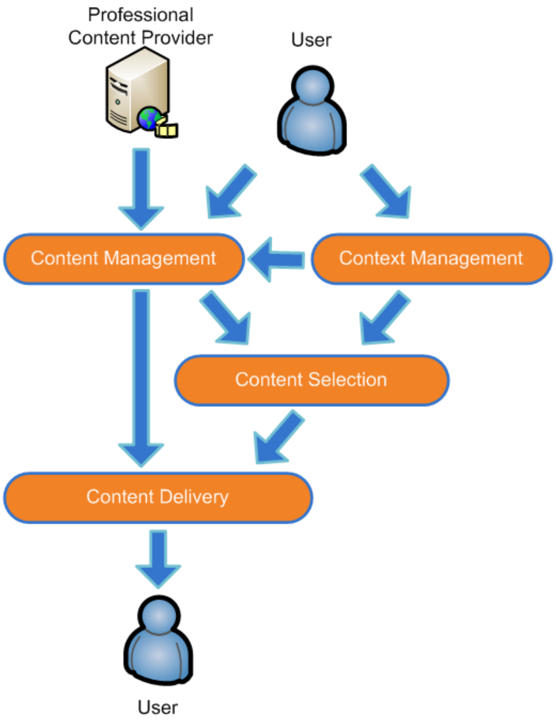

Figure 4.2: Overview of the Context-aware Content Rating System Architecture

4.3.3 Event-driven Federated Context Management

All the described CxMA enable the de-verticalization of context-aware applications, a key function of context-aware systems, but employ different paradigms and technologies in doing so. The most common case is having a request-response paradigm, which is typically implemented in recent years using Representational State Transfer (REST) approach. REST is a style for providing data services over HTTP (i.e. web services), where a Create/Remove/Update/Delete (CRUD) data operation is directly mapped to an HTTP request: the data resource is identified by the requested path, the operation by the request method, and the arguments for the create or update case are supplied in the request body. It is a minimalist approach to data services, using Domain Name System (DNS) for service discovery, not providing a service registry or an explicit interface definition.

Message-Oriented Middleware (MOM) is another architectural paradigm which had significant attention and dissemination, but that has been recently somewhat forgotten due to the massive adoption of HTTP-based web services. A MOM infrastructure, such as Java Message Service (JMS) [Hapner et al. 2002], allows diverse software components to communicate asynchronously. A coordinating component, usually called message broker, will handle endpoint resolution, message persistence and routing. The most striking difference between MOM and traditional web service is the messaging model: web services normally use the request-response model, while MOM supports more flexible and generic asynchronous messaging, which includes the publish-subscribe model.

As referred in Section 3.3.5, XMPP has been adapted for applications other than IM, such as VoIP [Ludwig et al. 2009] and microblogging [Saint-Andre et al. 2012],

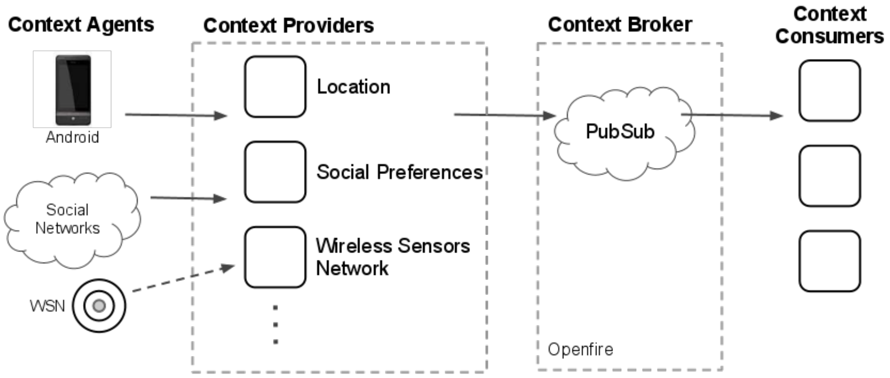

Figure 4.3: Global Architecture and Context Flow

and was recently proposed to be used for sensor control [Waher 2013]. Also, it can be used as a lightweight approach to MOM, more interoperable and dodging technological lock-ins of proprietary systems. However, unlike a typical enterprise MOM, it does not provide transaction management and may be less scalable.

In order to meet the context delivery latency requirements identified in Section 4.2.2, an event-driven context management platform was developed, building upon the learned lessons of the C-CAST context management architecture. The XCoA platform [Gomes et al. 2010] uses XMPP as the main communication protocol because it responds to several requirements identified in the previous section, such as federation and PubSub [Millard, Saint-Andre, and Meijer 2010], through the direct use of an existing standard. The extensibility of XMPP is one of its most important features, since it can be extended to support context information exchange.

Figure 4.3 shows the global architecture with the PubSub and XMPP elements involved. Context agents, posteriorly renamed to Context Source (CxS) to be consistent with other CxMA, can be very diverse - from sensors in mobile devices to social network profiles. Some CxS can be specific to a CxP as the Wireless Sensors Network Provider that communicate using a specific protocol. In the typical case CxP receives context information from CxS located on Android-based applications, which reads information from the available sensors, such as GPS, presence, mobile cell info, movement and luminosity.

In XCoA, the context information is sent from CxS - implemented as XMPP clients - on the user's terminals, sensors or networks connecting to CxP. The CxP listen for a specific context type from any agent and are built on the concept of XMPP components - entities void of IM and presence functionality. Avoiding IM and presence packets avoids overhead, enabling CxP them to scale better. Finally, the CxC can be either XMPP clients or components depending on the number of enablers they intend to support. Some CxP can also be consumers (e.g. the Location CxP fetches GPS or mobile cell information from other CxP and then publish the corresponding civil address as its own context information). In Table 4.1 we can see the mapping between the CxS involved and the XMPP implementation used to represent them.

For the XMPP server we used Openfire which is open source and Java based. The choice was made not only because Openfire has already many XEP included, but also because Java is a very common programming language. One important feature is the support for federation mechanism, that permits server to server communication. Open-

Context Actor	XMPP Structure
Sources	Clients
Providers	Components
Consumers	Clients or Components

Table 4.1: Relationship between roles in context management and XMPP structures

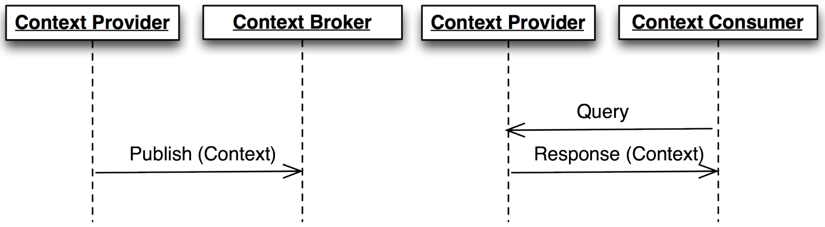

Figure 4.4: Context Consumption

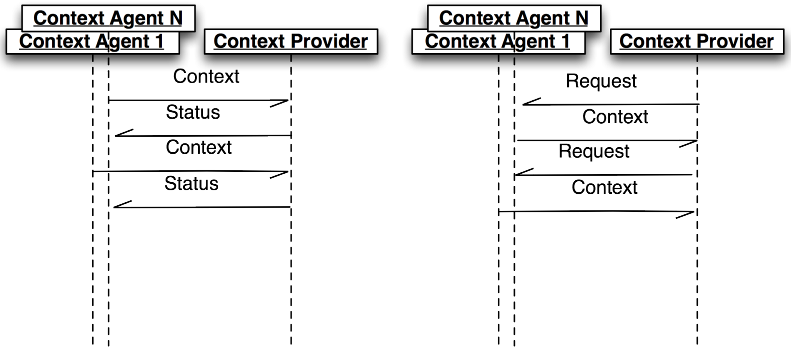

Figure 4.5: Context Acquisition

fire also allows to install or remove plugins in a very easy way and even develop new plugins, if needed, to add new functionalities. Most of the CxP are implemented in Java, using Smack as the XMPP library [Ignite Realtime 2002b]. All the CxP are external components, connected to the CxB - an XMPP server with PubSub functionality. CxP can either publish context information to the CxB, where context is cached and committed to a history repository, or listen for specific context queries that can be issued directly by CxC. These two communication schemes are presented in Figure 4.4.

We use IQ (Info/Query) XMPP stanzas for the communication between CxS and CxP, since it provide a simple structure for request-response interactions similar to the GET, POST, and PUT methods used on HTTP. Context information is collected from context agents through two different processes according to the nature and reliability of the context (Figure 4.5). The provider does the validation of the context information and then replies back with success or error. After receiving a valid XML, providers will publish consistent and aggregated information into the context broker. This intermediate step intends to address reliability and scalability concerns.

The described workflow cannot be used in all use-cases. As an example for social profile and social network providers we have resorted to external service providers:

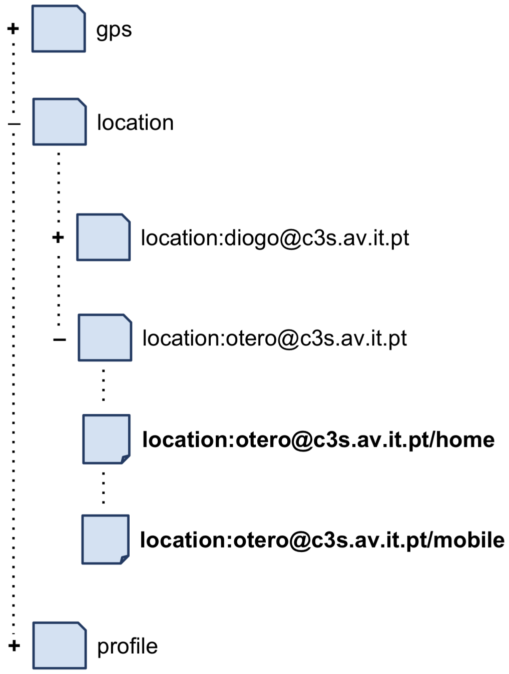
+
gps
–
location
+
location:diogo@c3s.av.it.pt
–
location:otero@c3s.av.it.pt
location:otero@c3s.av.it.pt/home
location:otero@c3s.av.it.pt/mobile
+
profile

Figure 4.6: Example of a Context PubSub Node Tree

Facebook and Orkut. These service provider offers a public API from which the developed providers can extract context information. These very specific CxP connect the service providers to the context management platform, proxying their information to the CxB. Information retrieved is then transferred to the CxB Cache and history using the same method described for the GPS use case.

CxC connects to the CxB in order to discover CxP. Context information is then retrieved directly from CxP through a polling mechanism or through a PubSub mechanism implemented by the CxB.

XMPP PubSub function is a relevant part of the platform, providing a framework of event notifications. There are two key elements in this model: the publisher and the subscriber, mediated by a service that receives publication requests and broadcasts event notifications to all subscribers. This allows the subscribers to receive context information without the need to poll the server. The service is contained in the broker's XMPP server and is also responsible on managing the entities authorized to publish or subscribe. All the information is stored in a *node* to which publishers send data that is then fetched by subscribers upon notification. The information is stored in a tree of two types of nodes:

- Collection nodes - can have more nodes inside but no published information;
- Leaf nodes - can be inside collection nodes and contain published data.

Regardless of node type, every node in the tree must have an unique name. Because of this limitation it was necessary to define some rules for the node creation. In Figure 4.6 is depicted part of a PubSub tree where we can see root nodes, that exist for every provider (location, GPS, profile, ...), inside of each we can create collection nodes identified by the name of it's parent - the CxP - concatenated with the unique identifier of the correspondent user.

Using XMPP allows the users to have multiple connected devices at the same time.

In Figure 4.6 the user *otero@c3s.av.it.pt* has published from two devices: *home* and *mobile*. For the leaf nodes we add the device identifier on where the context applies. Therefore, we can have a user with multiple context information for different devices, stored under leaf nodes identified by provider, user and device. In some cases, because of the nature of the provider, it doesn't make sense to have different context when the user publishes from different devices (e.g. social profile context) and so there's only a leaf node named *node@domain/default*. All CxC subscribing some user's context information should be aware not only of the correct CxP but also of what device to subscribe to. The subscription can be made anytime and the context information will be broadcasted to all subscribed clients or components.

Example 1 A Context Update from a GPS CxS

```
<iq type="set" to="gps.c3s.hng.av.it.pt" id="set1">
<query>
<gps xmlns="http://c3s.hng.av.it.pt/gps">
<latitude>45.21134</latitude>
<longitude>7.67054</longitude>
<accuracy>580</accuracy>
<altitude>19.3</altitude>
<bearing>18.3</bearing>
<speed>5</speed>
</gps>
</query>
</iq>
```

Example 1 shows the XML sent by the GPS CxS from an Android terminal to the GPS CxP. The presented XML is an XMPP IQ stanza the defines a request to be processed by the GPS provider. The provider does the validation of the context information and then replies back with success or error. After receiving a valid XML, providers will create (if not already present) the previously describe tree in the XMPP PubSub component, and publish the exact same information - in the example only whatever comes inside the <gps> node.

4.4 Disclosure Minimization in Context Information Systems

4.4.1 Location Disclosure Control

From the different types of context information currently used in services, location is the one that draws most attention since it is a very dynamic and relevant type of context. LBS have become increasingly more popular, taking as example popular web and smartphone location applications. Barkhuus and Dey [2003] had already published a case study back in 2003 that concluded that users are less concerned about their location being tracked as long as they found the service to be useful, and history seems to prove them right. Despite this significant success, there is still no comprehensive technological solution for adequately addressing privacy in systems that make use of context information. Access control in LBS is typically done by whitelisting users and other applications [Tsai et al. 2010], allowing them to access the location information. Furthermore, most of these applications require explicit user action for publishing information. The user has to say where he is from a location-aware list of places, an action commonly referred to as a *check-in*. This is also a form of privacy protection since permanently tracking the user without further control is very intrusive. However, in an AmI scenario location information will be published not only to other people but also to the entities that control the devices around us, embedded in the environment. This implies two things: first, the *check-in* technique currently used in many LBS is not an option, and second, the latency performance requirements for the context distribution become tighter.

These methods are the most common ones but they are not the state of the art on location context privacy. Toch et al. [2009] and Benisch et al. [2010] consider a location privacy preference model that uses not only whitelists but also the location information value, time of day and date. In their study, Benisch et al. measure the accuracy with which different privacy settings are able to capture the subject's preferences. Results show that using detailed privacy preferences such as date, time and location values leads to a 3 time increase in the accuracy of the settings, compared to whitelist-based settings only.

4.4.2 Context Quality and Obfuscation

Controlling who accesses the information is not the only way to protect location data. For example, Ardagna et al. [2007] use obfuscation techniques, which consist of deliberately providing less precise or even erroneous information. There is much done regarding the definition of specific obfuscation techniques for each context type. However, addressing context privacy generically has not been thoroughly explored. Wishart, Henricksen, and Indulska [2007] present a generic model for obfuscation which is strikingly similar to the generalization techniques of PPDM introduced in Section 2.3. This type of obfuscation requires ontologies to be defined for each context type, as there are potentially different levels of detail that can be considered. Location can have many detail levels, such as "room", "building", "city", while other context information might be of binary nature only allow or deny its access.

Sheikh, Wegdam, and Sinderen [2008] takes a different approach on context privacy by considering Quality of Context (QoC) - indicators describing how closely a piece of context information relates to reality. Sheikh argues that privacy is managed as a compromise between the different QoC expectations of the stakeholders - context owner, source and requester. This approach is aligned with the generic identity and privacy approaches previously presented. Sheikh et al. identify five measures of QoC: precision, freshness, spatial resolution, temporal resolution and probability of correctness. The required QoC is specified per service or service situation based on these parameter, so that services are not provided with access to context of a higher quality than is needed for the functioning of the services - the minimal disclosure principle.

4.4.3 Access Control in Event-Driven Context Management Architecture

In an event-driven CxMA, such as XCoA, context is distributed by publishing to PubSub nodes to which CxC are subscribed. The nodes here play the role of resources: in a request-response case a request would be sent to a resource containing the targeted information. In traditional access control, such as described for the web in Section 3.4, the access decision is done per request based on the requesting subject, the action being performed, the targeted resource, and environment parameters such as date and time. However, in context distribution, in both for request-response and publish-subscribe cases, the resource is volatile: the values it contains change over time, in many cases

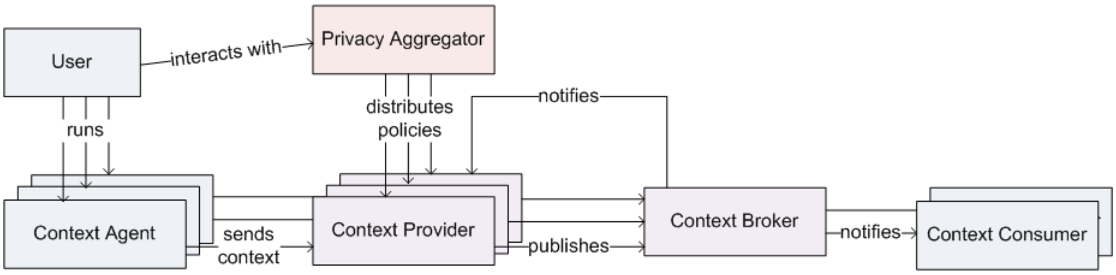

Figure 4.7: Architecture with Privacy-related Access Control

rather quickly. Since we are aiming at considering the context values themselves for the decision, not only the resource identifier, the traditional access control model needs to be extended. In addition to this, the real-time nature of the context distribution process cannot be debilitated by the implemented access control mechanism.

In order to address the problem of low-latency access control, the architecture initially presented by Gomes et al. [2010] was enhanced. This access control scheme supports decisions based on both resource value and metadata, as suggested by the privacy work of Toch et al. [2009]. The enhancement comprises of a new functional component, the Privacy Aggregator, depicted in Figure 4.7, and a few changes in existing components, namely in CxP and CxB. This component is the user's contact point for choosing privacy settings, and it is necessary for two main reasons. First, communicating the privacy setting implications to the user is an important problem [Sadeh et al. 2009] that needs to be tackled with specific solutions [Benisch et al. 2010]. Second, for the conception of the Privacy Aggregator relates to the concept and architectural definition of a CxP. Since different CxP may belong to different entities, and a user typically interacts with more than one CxP, having one of them accessing the privacy preferences meant to another CxP is not acceptable. The Privacy Aggregator works as a broker for specialized settings distribution. After the user sets his privacy options, the Privacy Aggregator is responsible for separating them per CxP and configuring them.

Furthermore, the Privacy Aggregator is bound to perform a key role in chaining different CxP for obfuscating context. From a CxP description of context inference and translation capabilities, the Privacy Aggregator can build relationships between the available context types. Some of these relationships will be obfuscations, and will replace the statically defined ontologies of previous work. For example, if a CxP exists that uses GPS location information to infer the city the user is in, then the Privacy Aggregator associates this with the GPS CxP and take it in account when asking the user for privacy settings for the GPS context type. The Privacy Aggregator should be controlled by the user or by some entity that the user trusts (e.g. IdP).

Not only is PubSub better than request-response for context dissemination, due to the real-time requirements of context-awareness scenarios, but also more flexible regarding access control. Request-response access control is done per request, and even if no environment parameters are considered - meaning that access decisions can be cached - there is always a check required per request. In publish-subscribe the access control can be enforced on subscription time, which happens typically a small fraction of the number times that context is required. Adopting his approach required changes in the original CxB. The CxP will then filter and explode requests to the *nodes* that are supposed to receive them, acording to the privacy policy that the Privacy Aggregator supplied.

The flexibility of the privacy settings enabled by this scheme fit the user's privacy expectations better than the ones currently in use, enabling users concerned with privacy to share more [Sadeh et al. 2009] [Benisch et al. 2010]. Furthermore, a CxMA must have low context delivery latencies so that it can be used for adaptation scenarios. We believe that these two points are key enablers for the era of AmI. The low-latency access control scheme [Gonçalves, Gomes, and Aguiar 2012], introduced here and detailed in Section 4.5, is a relevant contribution to the work presented in this thesis.

4.5 Low-Latency Access Control

4.5.1 Description

The access control scheme introduced in Section 4.4.3 enables real-time value and metadata based access control in an event-driven CxMA. Towards that goal, the concept of Context Profile was introduced, to ease the definition of the context privacy settings. A Context Profile refers to a context type and some optional privacy parameters: conditions expressing the values, dates and times for which the information can published, and an optional publishing delay. Then, in his privacy settings, the user associates each context profile to groups of entities that may be interested in taking the role of CxC. It is possible to define several Context Profiles for the same context type, even with privacy settings that are not mutually exclusive. Consequently the same context information may be distributed under different context profiles. Since the access control is done at subscription time, each context profile will necessarily correspond to a different publish-subscribe node, even if the same information is being published. While this brings an increase in the number of required *nodes*, or resources, and some replication of information, it will also reduce the context dissemination latency. It is a slight trade-off from horizontal scalability - the same server with the same processing power will typically support less users and load - to latency performance - context change notifications are as real-time as possible. By making this design choice, the only access control processing required at publishing time is the part of it that makes use of contextual information: context values, date and time of day.

The most relevant sub-components and interactions are depicted in Figure 4.8. The Privacy Aggregator provides the Context Profiles and associated users or user groups to the appropriate CxP, which implied changes in the original CxP. Since a Context Profile is context type specific it must be supplied to the CxP that publish that type of context information, and only to those. The CxP is responsible for managing the publish-subscribe nodes it publishes to. It must create and destroy them, based on privacy configuration changes, and manage its associated access control policies - it plays the role of an XACML PAP. It also is responsible for the contextual checks required for discovering the appropriate nodes where to publish. This last process happens once per context update. The CxB only needs to enforce the defined node access control policies, both when discovering and subscribing to nodes. It plays both the PDP and PEP roles, although these may be decoupled.

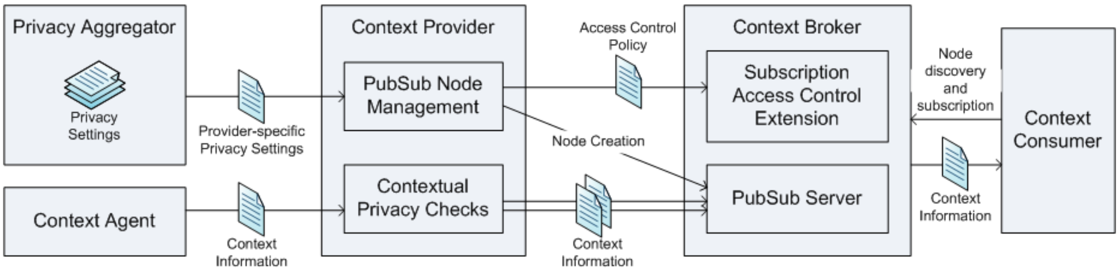

Figure 4.8: Design specification based on cardinality relationships between context update, subscription and consumption

4.5.2 Implementation

A prototype of the described system was implemented in order to demonstrate that it is possible to use complex privacy settings in context distribution without relevantly impacting the delivery latency and scalability. For this purposed we focused on the context distribution elements of the architecture because these are the ones that have an impact in the context delivery latency an that face the most relevant scalability challenges. The Privacy Aggregator was minimally implemented, only providing the specialized privacy settings XML to the Provider. The components were implemented based on existing and new libraries. The implemented architectural components and main implementation modules are depicted in Figure 4.9. The Context Model is the module that allows parsing and understanding context information and it can be extended for different types of context. The Context Privacy Model is the module that allows parsing and understanding the defined context privacy settings.

The context privacy settings define context profiles, as explained before. In the Context Privacy Model implementation XML was used to serialize and transport the settings. The settings represent conditions to be matched to context values, date and time, in order to evaluate whether some context update is to be published under that profile or not. Although an extension mechanism was put in place for representing these conditions, in this implementation only regular expressions were used. An example of the preferences file is shown in Example 2.

In this example there are two GPS location profiles defined. The first one publishes location only in if the location is within certain boundaries, in this case nearby the city of Aveiro, where the user lives as depicted in Figure 4.10. The second profile publishes

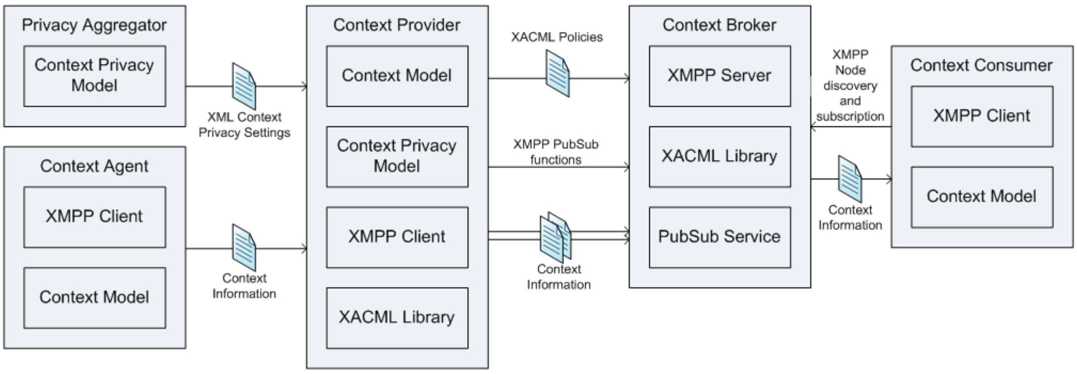

Figure 4.9: Main implementation modules

GPS location within a certain date/time window: from 9:00AM to 19:59PM, from Monday to Friday. The first profile is made available to the user's home appliances (air conditioning, water heating, ...), here identified by *home@openfire*, for them to be able to detect when the user is coming home. The second profile is made available to his work colleagues, here represented by every entity in the *openfire* domain.

Example 2 Context Privacy Settings XML Representation

```
<?xml version="1.0" encoding="UTF-8"?>
<privacy user="jmgonc@openfire" xmlns="http://iex.ptin.pt/ctx/privacy">
  <privacyProfiles>
    <profile id="1" name="GPS Tracking for Home Appliances">
      <publishedContextNamespace>http://iex.ptin.pt/ctx/gps</publishedContextNamespace>
      <parameterRules>
        <parameterRule>
          <parameter>latitude</parameter>
          <condition lang="regexp" var="">40\.6[2-5]\d*</condition>
        </parameterRule>
        <parameterRule>
          <parameter>longitude</parameter>
          <condition lang="regexp" var="">-8\.6[2-7]\d*</condition>
        </parameterRule>
      </parameterRules>
      <timeRule>
        <timeOfDayCondition lang="regexp" var="">.*</timeOfDayCondition>
        <weekdayCondition lang="regexp" var="">.*</weekdayCondition>
        <dailyExceptionCondition lang="regexp" var="">0</dailyExceptionCondition>
      </timeRule>
      <publishingDelay>0</publishingDelay>
    </profile>
    <profile id="2" name="Friends Place Tracking">
      <publishedContextNamespace>http://iex.ptin.pt/ctx/gps</publishedContextNamespace>
      <parameterRules>
      </parameterRules>
      <timeRule>
        <timeOfDayCondition lang="regexp" var="hour">9|1\d</timeOfDayCondition>
        <weekdayCondition lang="regexp" var="weekday">[2-5]</weekdayCondition>
        <dailyExceptionCondition lang="regexp" var="day">0</dailyExceptionCondition>
      </timeRule>
      <publishingDelay>0</publishingDelay>
    </profile>
  </privacyProfiles>
  <accessGroups>
    <accessGroup id="1" name="Home Appliances">home@openfire</accessGroup>
    <accessGroup id="2" name="Work Colleagues">openfire</accessGroup>
  </accessGroups>
  <profileGrouplinks>
    <link groupId="1" profileId="1"/>
    <link groupId="2" profileId="2"/>
  </profileGrouplinks>
</privacy>
```

The CxP was implemented using Java SE 6 and two existing Java open source libraries: Smack 3.2.0 [Ignite Realtime 2002b] and Sun XACML 1.2 [Sun n.d.]. The implementation is able to interpret the context privacy settings, and to create PubSub nodes and associated access policies in XACML which are supplied to the XMPP Server. The XACML policy only defines which users are allowed to perform a *read* action on a given resource (PubSub node). When context updates come in from Context Sources, the provider identifies which are the suitable nodes to which this information is published, first by checking the entity to which the context refers to, and then by enforcing the necessary parameter checks on that context information.

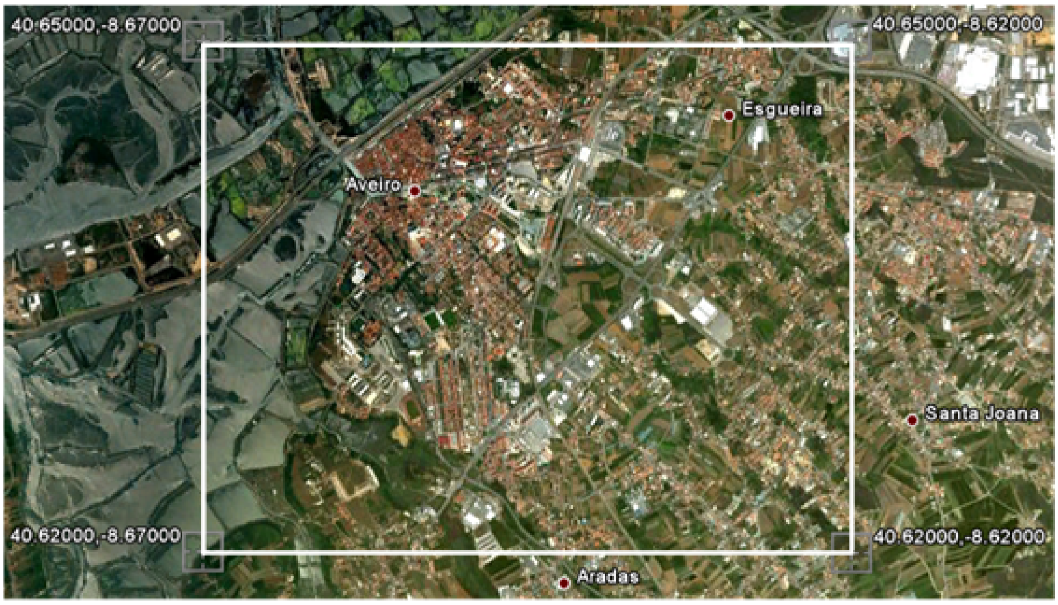

Figure 4.10: Area in which GPS Location is published for the first Context Profile

The CxB is implemented using Openfire [Ignite Realtime 2002a], which defines a plugin architecture that makes it easy to enforce access control on node discovery and subscription. Such a plugin was coded, also using the open source Java library Sun XACML 1.2. The policy for each node is loaded by the plugin to a simple PDP implementation. Whenever a discovery request for PubSub nodes or a subscription request arrives, the user and resource information are passed to the PDP in order to get a decision on whether a resource is accessible or visible to that user.

4.5.3 Performance Validation

In order to evaluate the performance impact of the implemented access control scheme, a testbed of virtual machines was setup. The performance metrics considered were processor load and end-to-end latency, in order to demonstrated that the implemented access control enabled system exibits the following key characteristics:

- does not significantly impact the scalability of the system - the processor load should only increase by a fraction of the original;
- is suitable for AmI adaptation scenarios - the introduced latency should be a fraction of the human visual reaction time of 190ms.

The host machine is an Intel Core i7 with 12Gb of RAM running VMWare ESXi 3.5. Four virtual machines were created with 512MB of RAM and a single virtual core, to ease the processor load measurements. In all of them Ubuntu Linux 11.04 Server edition was installed. Each of the four machines runs one of the components: CxS, CxP, CxB and CxC. For the CxS a simple Java-based XMPP client was coded, that generates random location context at a configured rate. Similarly, the CxS is a Java-based XMPP client that subscribes to the target PubSub nodes and writes to a file the received context marked with a timestamp. The CxB and CxP were already described. The baseline CxP is a simple provider that publishes every context that receives to nodes that it has configured without any further processing. The CxS and CxC are synchronized automatically before each test using a local NTP server.

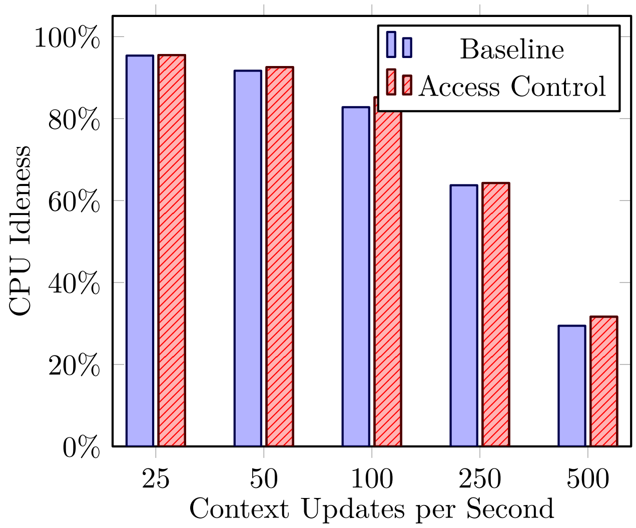

Figure 4.11: Context Provider Average Processor Idleness as Load Increases

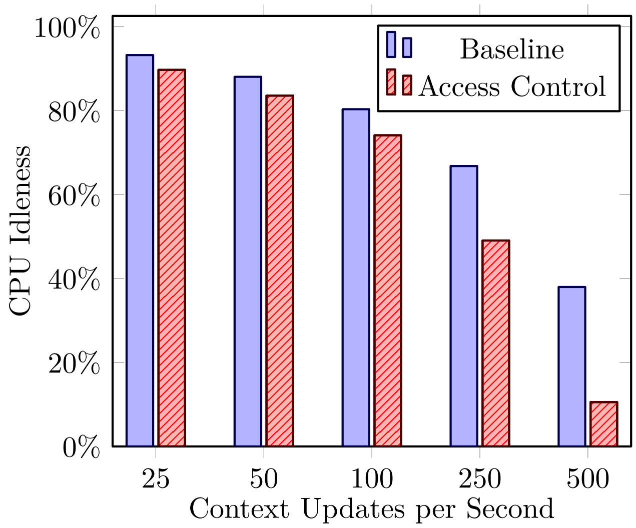

Figure 4.12: Context Broker Average Processor Idleness as Load Increases

In each test session a number of CxS published context at a fixed rate, and the CxC got that content and wrote it with timestamps to a file. Furthermore, the processor usage in both the CxB and CxP was measured, for both access control and baseline cases. The processor measurements are based on the idle processor output from vmstat [H. Ware and Frédérick n.d.]. The output shows average values for a sampling period that was set to 2 seconds. Since all the virtual machines only have one core, we don't have to worry about multi-core processor measurement issues. The result gathering was repeated in 5 sessions to detect odd events. Tests show that the same behaviour was observed in all test sessions, with relative standard deviation well below 10% for all cases, except in CxB processor measurements with 500 context updates per second on the access control case. In this case the relative standard deviation reaches almost 15%, due to the CxB not being able to handle all the load at times. In fact, the CxB processing load at around 500 contexts updates per second was the encountered

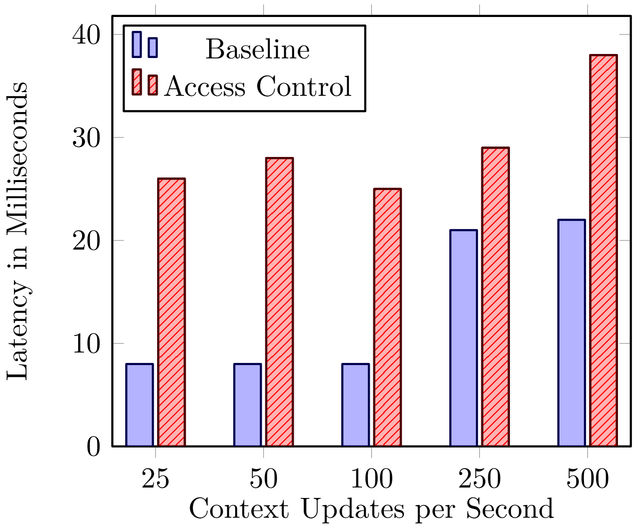

Figure 4.13: End-to-End Context Delivery Latency in Milliseconds with Load Increases

bottleneck for the tested deployment. Figures 4.11, 4.12 and 4.13 show the relevant findings.

As we test with higher load, the average processor occupation rises linearly, both for the CxP, as seen in Figure 4.11, and for the CxB, shown in Figure 4.12. In fact, in the CxP case, the average processor occupation is practically the same in both implementations. The only difference is a slightly larger memory footprint of the Access Control CxP. In the CxB, however, the linear increase in processing demand for the access control case is clearly faster than for the original implementation.

To properly analyse the rise in latencies, we have removed the latency data referring to the first 2 minutes of each session, both for original and access control cases. The reasoning for this is that the system takes some amount of time, in every case under 2 minutes, to stabilize its performance. We came to this value from the processor measurements, which show substantially higher loads in the first seconds of each session. Furthermore, since this is meant to be a system that is always running, the relevant results are the ones we obtain after the start-up. The results are depicted in Figure 4.13, which shows that context submitted to access control clearly takes more time to reach the destination, under any load. However this additional delay is estimated in around 20ms, a value perfectly in line within the human perception of *real-time*, representing roughly 10% of the human visual reaction time of 190ms. A bottleneck on the Context Broker was detected when load increases above certain values, however this is not relevant for the presented results as performance only starts being affected with loads above 500 requests per second.

4.6 Conclusions

Context-awareness is a key aspect of the AmI vision and distinguishes itself from work in M2M and IoT by its reactive nature. The technical feasibility of two flexible scenarios has been validated by using a context management platform integrated in a service-oriented ecosystem, within the scope of this thesis [Simões et al. 2009; Gonçalves, Delahaye, and Lamorte 2010]. While pre-existing work in context management targeted the functions necessary to deliver these future services, namely by decoupling context acquisition from consumption, it did not recognize the importance of the reactivity aspect in these systems. For that reason, a new event-oriented architecture is presented and validated with an implementation [Gomes et al. 2010].

Furthermore, the context-specific privacy issue of aligning information that is published and consumed was targeted. By extending the proposed event-oriented architecture, a low-latency access control system was developed. The system is capable of distributing context information in a privacy-friendly way, while it fulfils the real-time requirements of the context distribution process. The system considers fine-grained context privacy settings, allowing the user to set the context type and the valid parameters for which information should be published.

Further work in this track should include complex access control effects that could be implemented with probabilistic comparison functions. For example, a profile might be created that allows GPS updates based on a probabilistic distribution centred on some coordinates, result on a *fade effect* of the updates as the user moves away from those coordinates. Another work track relates with the inclusion of parametrizable obfuscation CxPs in the platform, configured by the Privacy Aggregator, and the use of additional QoC metrics for the access control decision.

Chapter Five

Data Perspective

Data analysis techniques that enable re-identification, as well as existing countermeasures, are presented. The limitations of current dataset sanitization techniques are identified, namely the issues with the high-dimensional case. One of the most relevant contributions to the state-of-the-art presented in this thesis is a sanitization technique that works in the high-dimensional case, and is discussed in this chapter.

5.1 Introduction

5.1.1 Personal Data Aggregation

Personal data aggregation is at the centre of the digital economy. Consumption profiles are build in order to deliver targeted advertising, recommendations and even to be sold as a commodity. Despite obtaining revenue directly from the use or sale of personal data being new, data aggregation problems have been discussed already since the 1970's. A number of government agencies and private companies, such as credit bureaus, have long made use of personal information to conduct their activities. The census are an example of personal data aggregation by a government agency which puts the public interest in collision course with individual privacy. Using an Statistical Database (SDB) it is possible to harmonize these two competing requirements, exposing the census data only through aggregate queries - calculate means and sums. However, even accessing only the aggregated view of data, it is possible to extract information regarding specific subjects [Adam and Worthmann 1989].

Today, the focus is more directed to data mining. User behavioural information of product and movie ratings, social network friends and *likes*, search terms, purchases and website visits are used to devise behaviour profiles that can be used for recommendations, targeted advertising or identifying a business opportunity. The field of Privacy-Preserving Data Mining (PPDM) aims to address privacy when data is used or made available for these purposes. The data used in these scenarios is typically made available to third parties in an supposedly anonymized form. However, the employed anonymization mechanisms are usually naive, relying on the replacement or deletion of common identifiers like name and email address. Such methods are vulnerable to re-identification attacks using information that is apparently harmless, such as zip code, sex and birth date. Sweeney determined that with those three attributes it is possible to identify 87% of the US population [Sweeney 2000]. Other notable examples of supposedly anonymized data releases which prompted legal and public-relations problems for the involved companies are the AOL search queries and the Netflix Prize case, as described in Section 2.1.3.

For the Netflix Prize data mining competition a dataset was released for participants to use, containing the ratings that 480 thousand users gave to 17 thousand movies as well as the dates in which the rating was given. The user's identification information was suppressed in order to anonymize the dataset, leaving only a meaningless user id number. In 2008 Narayanan and Shmatikov successfully re-identified a number of users in the Netflix dataset by cross referencing that information with information crawled from IMDb, showing that the dataset was vulnerable to privacy attacks [Narayanan and Shmatikov 2008].

Restricting access to gathered personal data is an exercise of balancing of two contradictory requirements: the privacy of the subjects in the dataset and the *utility* of analysing the data. Perfect privacy is achieved by destroying the data, while utility can be maximized by publicly releasing all the data. Normally neither extreme happens, and the data is made available via aggregate queries or after some sanatization process (such as naïve anonymization) is performed. Independently of the case, this privacy-utility trade-off is of key importance for the privacy protection mechanism.

5.1.2 Chapter Outline

In Chapter 3 the communications related issues were addressed, namely techniques that allow communicating personal information that refers to the same subject in a way that it its unlinked to him and to other information communicated about him. However, using context information referring to the same subject, it is possible to bypass these PETs by identifying the subject to which some information refers to, based only on data analysis. These re-identification data-centric techniques are mainly addressed in the bodies of knowledge identified in Section 2.3.4: PPDM and SDC.

In this Chapter the models and theoretical foundations of these fields are presented, and existing data-centric privacy preserving techniques are discussed. Also a communications-inspired re-identification countermeasure is presented, which represents a major contribution of the work presented with this thesis. This countermeasure fits the privacy-preserving data publishing assumptions and targets the high-dimensional case, in which the each user may have information available for a very large number of attributes, as it happens in context-aware systems.

5.2 Models and Foundations

5.2.1 Concepts and Models for Data Privacy

Privacy, in the context of datasets containing personal information, typically has an adversary that uses the access to the database and some auxiliar, typically public, information on the target subjects, in order to get more information about them. The attack can be performed in two different ways:

- by matching a dataset record with a known subject, re-identifying that record;
- by retrieving some unknown potentially sensitive data about a subject, disclosing that attribute.

The re-identification of the record obviously implies the disclosure of all the attribues in the record, however it requires the adversary to sufficiently isolate the record from all others, based on the available auxiliary information. An attack at the attribute level, while rendering less rewards for an adversary, is less demanding than an identification. It simply requires the set of match-candidate records, based on the available auxiliary information, to have a distribution of values for the target attribute that enables value inference with high enough probability. Some literature also considers that detecting the presence of a user in a database, even if not devising the specific record that corresponds to him, also constitutes a privacy harm, especially it the released database is of sensible nature [Nergiz, M. Atzori, and Clifton 2007].

In order to enable mathematical abstractions, data is usually modeled as a matrix where each row, or record, refers to a subject and each column, or dimension, to an attribute. This means that each dataset record, referring to a subject, can be represented as a point in multi-dimensional space. The goal of a re-identification attack adversary, sometimes designated as "isolator" [Chawla et al. 2005], is to "single out" a point in this multi-dimensional space. Chawla et al. [2005] mathematically formalized this goal. For an isolator I, a dataset D of n points in m-dimensional space, and an auxiliary information z, let $I(D, z) = q$. Let σ be the the distance to the dataset point x nearest to q. Let $B(p, r)$ be an m-dimensional ball of radius r around point p. Consider now two parameters: an isolation parameter c and a privacy threshold t.

If the m-dimensional ball of radius $c \times \sigma$ and centered at q contains at least t dataset points, that is $|D \bigcap B(q, c \times \sigma)| \geq t$, then the isolator fails, otherwise it succeeds. This definition does not consider isolation in a few dimensions, as the authors note. An extended definition involves projecting the points of D in a k-dimensional hyperplane, with $k \leq m$, and calculating the isolation in the hyperplane.

Let's similarly define *sanitizer*: an algorithm that takes some dataset D, a set of n points in m-dimensional space, and outputs a dataset D' with some number of n' points in a possibly different m'-dimensional space. Most of the solutions presented in the PPDM field can be considered sanitizers. Their objective is that the resulting dataset D' is more private than the original, with a moderate cost of utility. However both privacy and utility are significantly context dependent and difficult to quantify.

The vulnerability to re-identification of a dataset, sanitized or not, can be estimated as a probability of isolation on a dataset D given some auxiliary information z and parameters c and t. The auxiliary information and parametrization is highly dependent on the attack model: they represent the previous knowledge of the adversary and his goal when attacking the dataset.

The utility of a dataset, sanitized or not, depends on the purpose for which it is used. There are several possible purposes, namely predicting unknown values or classifying records. Some processing workload is applied on the data so that the required information is calculated or predicted. However, when sanitizing a dataset the workload is not known, making it difficult to generically evaluate proposed sanitizers. Some work uses some proxy metrics to estimate the loss of utility, which typically aim at minimizing the changes done from the original to the sanitized dataset. Others measure the loss of utility empirically by considering the error of statistical aggregates. However, the utility metrics that give best applicability guarantees are those which evaluate the impact on common data-mining workloads [Brickell and Shmatikov 2008]. With the popularization of recommendation systems a common workload involves estimating the values of empty attributes for each record.

As referred in Section 2.3.4, Dwork's Differential Privacy [2006] represents a strong mathematical foundation for data-privacy work, which worked as the bases for much new work in the area in recent years [Dwork 2011]. In Differential Privacy, Dwork formally defines a very strong privacy guarantee, which implies that it is not sufficiently distinguishable whether any given record is part of the database or not.

5.2.2 From k-Anonymity to t-Closeness

The work by Sweeney on k-Anonymity [2002] is probably the most common reference in PPDM. It coins the terms "quasi-identifier" and "equivalence classes". Quasi-identifiers are attributes which alone do not identify the user, but used together can be leveraged to do so. These attributes are typically easy to obtain by other means, and therefore considered to be part of the adversary's auxiliary information. Examples of such attributes are the previously referred zip code, sex and birth date (see Section 5.1.1). Opposite to quasi-identifiers, a dataset also contains sensitive attributes, the ones that the adversary aims at discovering the value.

Informally, a dataset satisfies k-Anonymity if and only if for each record of the data set there are at least k-1 other record with the same quasi-identifier values. This way, the adversary cannot distinguish which of the k records belongs to the target subject. In order to enforce this, the quasi-identifier values are generalized, masking their real values with more generic ones when necessary. These groups of at least k elements, in which rows are indistinguishable regarding their quasi-identifiers, are called equivalence classes. k-Anonymity effectively targets the quasi-identifiers, improving resilience against re-identification attacks, but disregards the sensitive attributes.

A follow up approach dubbed l-Diversity [Machanavajjhala et al. 2007] captures this shortcoming by presenting an approach that resists to two types of attacks to which k-Anonymity is vulnerable: the Homogeneity and the Background Knowledge attack. In these attacks sensitive attributes can be leaked even if the adversary cannot associate the individual with a single row of the equivalence class, it just requires that the sensitive values are not diverse enough. For example, if all the records in the target equivalence class have the same value for a sensitive attribute then there is sensitive attribute disclosure.

N. Li, T. Li, and Venkatasubramanian [2007] further analysed these issues and establish a privacy model that formalizes the privacy breach as the change of knowledge of the adversary as he comes in contact with a dataset. This approach, dubbed t-Closeness, considers three adversary information states:

1. the adversary's prior belief (auxiliary information),
2. the adversary's belief after knowing the overall distribution on sensitive attributes in the released database,
3. the adversary's belief after knowing the distribution on sensitive attributes of the rows that match the target person.

The information state 2 has more information than 1, and is especially relevant to presence privacy cases, such as in [Nergiz, M. Atzori, and Clifton 2007]. However, since this only applies to a small subset of cases, Li et al. assume that the overall distribution of sensitive attributes is very similar to the one from the global population, which configures public data, and disregard the information state change between 1 and 2. Consequently t-Closeness focuses on protecting privacy by reducing the difference of information between information states 2 and 3. This implies approximating the distributions of sensitive attributes of each equivalence class to the overall sensitive attributes distribution. It is not enough that the sensitive attributes are diverse for each equivalence class, as l-Diversity states, but that their sensitive value distribution should is similar enough to the overall sensitive value distribution. This is justified by the skewness attack: if the overall probability of an individually having some disease is 1%, and inside the target equivalence class half of the subjects have that disease, then the adversary managed to gather significant information about the target subject.

5.2.3 High-Dimensional Datasets

Dataset can be classified regarding their dimensionality, based on the multi-dimensional space abstraction: in case it has few attributes it's a low-dimensional dataset, while if it has many attributes it is high-dimensional. An example of a low-dimensional dataset would be the yellow pages (name, address and phone number), while an example of an high-dimensional dataset is the Netflix dataset, in which each of the 17 thousand movies is a different attribute and the rating is the value. Such datasets with thousands of attributes are usually sparse: each record typically has a (non-null) value defined only for a small fraction of the attributes. The number of non-null values in a record or attribute is denoted as support of that record or attribute. Another common characteristic of high-dimensional datasets is that the distribution of the attribute support is typically long-tailed: there is a small number of attributes that have non-null values for many records while there is a large number of attributes that only have non-null values for a few records. A side effect of this is that records are very distinguishable, even by merely considering which attributes are defined and which ones aren't, representing an anonymity threat even if attribute values are obfuscated or omitted [Narayanan and Shmatikov 2008; C. C. Aggarwal 2005].

5.2.4 The Quasi-Identifier Assumption

Most work in PPDM relies on the assumption that attributes can be classified as quasi-identifying or sensitive, where quasi-identifiers are attributes that are relatively easy to gather from other sources - which compose the adversary's auxiliary information - and sensitive attributes are the target of the privacy attack. However, in many situations the quasi-identifier and sensitive attribute separation cannot be clearly defined. Considering diverse real life scenarios, the sensitive attributes in one case may not be sensitive in another case: an individual's home address is sensitive information in a database of high profile art collectors, while it is a quasi-identifier in most other databases. Also, without assuming limitations on the adversary's access to information about an individual, any big enough set of attributes can be considered quasi-identifier as together the attributes are likely to re-identify that individual.

Re-identification attacks are usually agnostic to the semantics of the attributes and rely instead on two properties that are common to many types of personal information [Narayanan and Shmatikov 2010]. First is the stability of data across time, enabling datasets that are not temporally coincident to be used together in re-identification, and thus making it easier to have available auxiliary information. Secondly, if the quantity and precision of the data attributes is high enough, then it becomes highly unlikely that two individuals have the same set of values. This is especially easy in the high-dimensional case, prompting the discussion of what personally identifiable information truly is, and whether any type of information can be distinguished between personally identifiable and non-identifiable simply by its semantic.

Regarding the sensitivity of attributes in high-dimensional datasets, e.g. the movies rated and the items bought, while some movies/items have more potential to promote privacy harms than others, it is not clear which attributes are sensitive and which may be part of the auxiliary information. They are potentially all sensitive depending on the disclosure context: buddies would potentially crack jokes if they knew the rating given to some musical movie or the future employer could have second thoughts about hiring if he knew the rating given to certain ideology-charged movies, and so on.

5.3 Privacy-Perserving Data Mining Sanitization Techniques

5.3.1 Existing Sanitization Techniques

The concepts of k-Anonymity and t-Closeness are privacy conditions, goals to be achieved by sanitizers. It is generally assumed that all sanitizers perform record order randomization so that no information is contained in the order by which records are presented in the dataset. A sanitizer typically use one or two types of operations on a dataset in order to reach the defined privacy guarantees. The following types of operations can found in literature:

- generalization: values of attributes are changed to a more general version of the value (e.g. birth date attribute is changed to birth year);
- suppression: records or values which are very distinguishable are simply removed from the dataset;
- forgery or synthetic data generation: generated records or values are added to the dataset;
- perturbation: noise is introduced in the individual value of the attributes, which can be cancelled out when retrieving an aggregate result;
- swapping: exchanging sensitive values between records while maintaining statistical properties;
- partitioning: records (horizontal partitioning) or attributes (vertical partitioning) are separated.

Suppression and generalization are the two techniques proposed by the original k-Anonymity work [Samarati and Sweeney 1998], in order to achieve the defined privacy condition. Generalization is a technique used also in context obfuscation, as explained in Section 4.4.2, which transforms a value in a more general version of that value, according to some domain hierarchy. As generalization reduces dataset utility, the objective is usually to meet k-Anonymity, or other privacy goal, while minimizing the amount of generalization done. As a consequence of this, and also because they require a domain-specific hierarchy for each data type, generalization is not a method that can be transparently applied to any dataset: it typically requires a manual data analysis phase to build or apply domain hierarchies and to parametrize minimization.

Suppression is used typically as a last resource technique for dataset outliers. If generalization alone would be applied to satisfy some privacy goal, the presence of these outliers could force significantly more aggressive generalization, reducing the amount of information in most records, thus dataset utility. It usually proves more utility-friendly to drop the outliers altogether rather than to excessively generalize the whole dataset. In some situations it could be more utility-friendly to add synthetic data points, to help hiding some records uniqueness, than to suppress them. The data should be generated so that the resulting dataset maintains the statistical properties of the original dataset [Fung et al. 2010, p. 22].

Perturbation, also called additive noise in SDC literature [Fung et al. 2010, p. 22], works by altering individual values of some attribute, according to some known distribution, making it possible to recover generic statistical properties of the original data but difficult to recover original values since the noise introduced for a specific value is unknown [Dakshi Agrawal and C. C. Aggarwal 2001]. A variant of perturbation, inspired in synthetic data generation, called condensation [C. C. Aggarwal and Yu 2004], considers the relations between attribute values, and preserves the most relevant inter-attribute correlation data. The data is “condensed” in a predefined number of groups and then randomly re-generated based on each group’s statistical properties. This allows correlations between different groups to be preserved while making individual data records indistinguishable within the groups. Changing the number of groups allows to adjust the trade-off between anonymity and data utility.

Data swapping involves exchanging values of sensitive attributes among individual records while the swaps maintain low-order frequency counts, i.e. entries in the the marginal table. This introduces uncertainty about the true values of sensitive attribute value while maintaining key statistical properties of the dataset. The method originated in SDC [Dalenius and Reiss 1982] and has been only casually applied in the PPDM field [Fienberg and McIntyre 2004].

One of the advantages of partitioning-based techniques is that the resulting dataset values remain unchanged - what changes are the associations between them. The simplest forms of partitioning are atomization and permutation, which achieve k-Anonymity by separating the dataset in a quasi-identifier dataset and a sensitive dataset. The quasi-identifier dataset matches the records to a *GroupID*, and the sensitive dataset matches each *GroupID* to the sensitive attribute values [Fung et al. 2010, p. 20]. The groups of this approach are analogous to the equivalence classes in the traditional generalization approach of k-Anonymity. Also T. Li et al. [2012] propose *Slicing*: a vertical and horizontal partitioning method that complies with l-diversity.

5.3.2 High-Dimensional Sparse Dataset Anonymization

In Section 5.2.1 we defined sanitizer as an algorithm that takes a dataset and outputs another dataset, potentially with a different number of records and dimensions. Now let *anonymizer* be a sanitizer which specifically aims at protecting against re-identification of records. Some work has been done regarding the anonymization of sparse high-dimensional data. Ghinita, Tao, and Kalnis [2008] propose Correlation-aware Anonymization of High-dimensional Data (CAHD) to protect non-null occurrences of sensitive attributes in an high-dimensional dataset. The rationale is to form a group of similar records for each sensitive occurrence and associate the sensitive occurrence to a group rather than to a specific record. Yabu Xu et al. [2008] formulate the privacy problem in a way that allows them to relate some amount of auxiliary information with the probability of sensitive attribute disclosure, and propose a suppression-based algorithm so that the dataset complies with a privacy requirement formulated that way. In subsequent work [Yabo Xu et al. 2008] the concept of frequent itemsets are used in order to minimize the utility lost in the suppression process. However in all this work the quasi-identifier and sensitive information assumption is present. T. Li et al. [2012] argue that because vertical partitioning is used, slicing can be used in high-dimensional scenarios and test the algorithm on the Netflix dataset. However, as also noted by Manolis Terrovitis, Nikos Mamoulis, Liagouris, et al. [2012], *Slicing* cannot handle sparse data. For the Netflix validation performed by Li et al., the dataset's null values were replaced with the average rating of the movie, removing sparsity - the main source of distinguishability between records [Narayanan and Shmatikov 2008; C. C. Aggarwal 2005].

The high-dimensional case has also been targeted by privacy work that does not target data publishing, but instead interactive data access. Chawla et al. [2005] presents an important base in this field by considering all attributes as dimensions of a hyper-cube of records and formulating mathematical definitions for privacy and sanitization. Also, two sanitization methods are proposed: one that relies in histograms to transmit the data - coarsely groups records to provide relevant statistical information - and another that uses perturbation to make records less identifiable (or isolated, in their terminology). Promising work has been recently done towards achieving Differential Privacy [Dwork 2006] in high-dimensional datasets. McSherry and Mironov [2009] adapt the most common prediction techniques used for the Netflix Prize to return differentially private recommendations. The experimental results show impressive RMSE results, however the responses are differentially private regarding the detection of ratings and not users, which would require much more aggressive noise addition, as the authors themselves note. However, the interactive data access model that these approaches assume has fundamental implications on the adversary model and data applications, which differ from the data publishing model targeted in more detail within the scope of this thesis.

Most of the work that targets high-dimensional data publishing relies on the assumption that attributes can be classified either as quasi-identifying or sensitive. However, as discussed in Section 5.2.4, this assumption is rarely applicable in real scenarios. Unlike previously discussed high-dimensional data publishing work [Yabu Xu et al. 2008; Yabo Xu et al. 2008; Ghinita, Tao, and Kalnis 2008; T. Li et al. 2012], many other authors drop this assumption altogether in the high-dimensional case: any attribute can belong to the adversary's auxiliary information and all attributes are to be protected. Notably, Manolis Terrovitis, Nikos Mamoulis, and Kalnis [2008] proposed a new version of k-anonymity for set-valued high-dimensional data, k^m-anonymity, because k-anonymity assumes the existence of quasi-identifiers, and because the methods to achieve it do not scale to the high-dimensional case [Meyerson and Williams 2004]. Given an adversary with auxiliary information of at most m attributes about a record, a k^m-anonymous dataset must contain at least k records undistinguishable with respect to those attributes. The authors also describe a generalization-based method to make set-valued high-dimensional datasets k^m-anonymous. This privacy guarantee is also adopted in a cluster-based generalization technique [Gkoulalas-Divanis and Loukides 2012].

Recently a number partitioning-based techniques to address the high-dimensional case have been suggeted. R. Chen et al. [2011] describe a probabilistic top-down partitioning algorithm to generate differentially private data releases. Unlike most work done under Differential Privacy that considers an interactive approach to data access, Chen's goal is to publish a dataset via differential privacy. Also, in work following up the use of generalization in the high-dimensional case [Manolis Terrovitis, Nikos Mamoulis, and Kalnis 2008], Terrovitis et al. choose to use disassociation, a horizontal and vertical partitioning approach, to guarantee k^m-anonymity in a dataset of web query terms [Manolis Terrovitis, Nikos Mamoulis, Liagouris, et al. 2012]. Finally, Zakerzadeh, C. Aggarwal, and Barker [2014] published a vertical partitioning approach to achieve k-anonymity in high-dimensional datasets. The type of partitioning used differs from the one used by Manolis Terrovitis, Nikos Mamoulis, Liagouris, et al. [2012], as it is applied uniformly to all records. They note that while all the theoretical difficulties of the dimensionality curse [C. C. Aggarwal 2005] remain true, their impact can be reduced by relying on common properties of real-life datasets.

5.4 Privacy in Personalized Recommendations

5.4.1 Recommender Systems

The use of recommendation techniques in e-commerce sites is now widespread. Getting automatic recommendations for which items are worth looking at is essential when navigating a large search space. The term *collaborative filtering* was coined by the developers of one of the first recommender systems, and is commonly used to refer to such systems even if the system does not drive its users to collaborate explicitly [Su and Khoshgoftaar 2009]. In the context of recommender systems, dataset records represent users, attributes represent items, and the values usually are the ratings given by users to items.

Recommender systems can be functionally classified into three major groups [Gunawardana and Shani 2009]:

1. generic recommenders, which recommend sets of "good" items to the user;
2. utility optimization recommenders, a generic recommender tuned to the goals of the business implementing it;
3. prediction recomenders, which attempt to predict user opinion (i.e. rating) over a set of items.

Generic recommenders can be done based on aggregate data, not requiring access to the full dataset. Some web sites simply keep track of the rating average of each item and the aggregate number of ratings in order to produce "popularity-based" recommendations.

Unsurprisingly, most literature on recommender systems focuses on prediction recommenders. These rely on the assumption that if some users rate some items similarly, they will also rate other items in a similar way. In order to identify these similarities, prediction recommenders analyse large ratings datasets, such as the one from Netflix Prize [Su and Khoshgoftaar 2009]. Data mining is performed by the system on such high-dimensional datasets in order to estimate the missing values, which can be used to predict the rating that users would give to each item. Throughout this work let us refer to recommendations given by prediction recommenders as *personalized recommendations.*

5.4.2 Privacy in Recommender Systems

In the context of recommender systems, existing privacy work can be classified based on the topology of the recommender system: centralized or distributed. In the centralized case, the goal of privacy work is to keep the recommender system from knowing the exact rating while still providing with useful recommendations. Similarly to the work in privacy preserving data publishing, the recommender system, which may be the adversary, has unrestricted access to the dataset after it has been published.

Privacy work addressing centralized recommenders is similar to the work seen in privacy-preserving data publishing. Approaches typically rely in the application of some perturbation to the ratings given by users before they are supplied to the centralized entity. Polat and Du [2003] use perturbation, as do Berkovsky et al. [2007] along with simpler obfuscation techniques. Their privacy model aims to hide from the centralized recommender, with sufficient probability, the real rating the user provided to each item. However, these attack models do not consider auxiliary information.

In the case of distributed recommenders, a dataset of ratings given by numerous individual users is never collected and processed by a central entity. Users of such systems collaborate in a peer-to-peer manner in order to rate items such that the best rated items are recommended. The privacy goal here is keeping the values of ratings known only to the user that gave them. The adversaries are the other users that collaborate in rating the item. A well established approach for the peer-to-peer case is the use of some homomorphic encryption scheme in the collaborative filtering protocol, as do Canny [2002] and many others after him (e.g. Zhan et al. [2010] and Pathak and Raj [2011]). Homomorphic encryption enables a number of users sharing their encrypted ratings with each other and being able to retrieve the aggregate ratings.

Table 5.1: Recommender Privacy Scenarios

Privacy Scenario	Accessible Data	Recommender Applicability
Aggregate data release	Rating average and count per item	Generic recommendations
Interactive aggregate queries	Sanitized aggregate query responses	Generic recommendations
Distributed recommenders	Aggregate rating matrix	Personalized recommendations
High-dimensional data publishing	Sanitized high-dimensional dataset	Personalized recommendations

Furthermore, Canny [2002] describes some degree of personalization is possible using this scheme by locally correlating user preferences and the aggregate ratings model.

It's also possible to consider the interactive data access model in the context of recommender scenarios. In this case the attacker and the recommender also doesn't have access to the full dataset, only to aggregate queries performed on it. Differential Privacy, widely recognized in the data privacy community as a very strict privacy guarantee, is built on this model which is obviously capable of producing generic recommendations through aggregate results.

Table 5.1 synthesizes the applications of different privacy protection models to recommender scenarios, assuming that the recommendations and the adversary access data under the same model. A naïve case is also considered in which a trusted centralized recommender stores only anonymous item rating averages and vote count data. Generic recommendations are possible in a number of different scenarios, some of which provide significantly stricter privacy guarantees than the ones possible in a data publishing setting.

5.4.3 Utility Metrics in Privacy Preserving Data Publishing

Generic recommendations can be provided based on aggregate data alone, but personalized recommendations require complex data analysis, enabled, among other methods, by performing data mining on published rating data. However, privacy work under the data publishing attack model has consistently used utility metrics that capture generic statistical properties of datasets.

In order to illustrate this point, let us enumerate the utility metrics used in high-dimensional privacy-preserving data publishing work that doesn't rely on the quasi-identifier assumption, previously described in Sections 5.3.2. Manolis Terrovitis, Nikos Mamoulis, and Kalnis [2008] estimated the impact of their generalization method by using Normalized Certainty Penalty (NCP), which merely captures the degree of generalization the method enforces. Similarly, Gkoulalas-Divanis and Loukides [2012] rely on generalization-minimization utility measures which can be applied to non-hierarchical generalizations. All these techniques focus on the abstract measure of utility loss, failing to relate it to a dataset use application.

The utility metrics used in the most promising high-dimensional work mostly validate statistical aggregates of the dataset. R. Chen et al. [2011] evaluates utility through the relative error of counting queries. Manolis Terrovitis, Nikos Mamoulis, Liagouris, et al. [2012] rely on two different metrics:

1. top-K deviation: the ratio of the top-K frequent itemsets of the original dataset that appear in the top-K frequent itemsets of the anonymized data;
2. relative error in the support of term combinations, limited to combinations of size two.

Finally, Zakerzadeh, C. Aggarwal, and Barker [2014] measure utility in terms of changes in classification accuracy using a classification dataset [Chapman and Jain 1994] with 168 attributes.

Table **??** synthesizes the used privacy metrics in previous work. Having applicability in mind, utility must be evaluated through the analysis of increased error in typical workload results, and should not be a secondary performance metric. Generic recommendations are possible without the collection and publishing of data. These practices are usually justified by functionality that is not possible to achieve with access to aggregate data alone.

5.4.4 Personalization Utility

A realistic measure of utility in personalized recommendation scenarios is the prediction error of data mining algorithms used to perform them. The evaluation process of such algorithms usually involves splitting the dataset into a training set and a test set, running the algorithm on the training set to try and predict the values of the test set. The error can be measured in terms of root mean square error (RMSE) of the predicted values compared to the real values. While this measure typically evaluates the prediction performance of the algorithm, when the same algorithm is used against two related datasets, the original and a sanitized version, the utility loss incurred in the sanitization process can be estimated.

In the context of personalized recommendations a utility baseline must be considered: the utility of performing recommendations based on aggregate data. If the utility loss of a sanitization process brings the RMSE of predictions to the values that can be achieved by making naïve predictions based on aggregate data, then the sanitization process is useless as it makes more sense releasing aggregates than the dataset. For this reason, a new utility metric that enables us to measure the utility of datasets over this baseline value is proposed.

Let us formally define Personalization Utility. Let P be the prediction function of a personalized recommender system, and A a naïve prediction function which predicts that all users rated items with the average rating given to that item. Let now $RMSE(P, D)$ be the RMSE resulting from applying prediction function P to dataset D, and $RMSE(A, D)$ be the RMSE of using impersonal rating function A to predict ratings in dataset D.Then, Personalization Utility of prediction function P for dataset D, $\mu(P, D)$, captures the degree to which P adapts to the preferences of individual users in dataset D:

$$\mu(P, D) = 1 - (RMSE(P, D)/RMSE(A, D))$$

This new utility metric enables the comparison of sanitization processes to be applied in recommendation data publishing scenarios. $\mu(P, D)$ is positive if personalization benefits predictions, and is proportional to the importance of personalization in the recommendation.

Because data publishing is primarily justifiable in personalized recommendation scenarios, a minimum acceptable value for utility must be considered: the utility provided by recommendations based on aggregate data. More formally, for a sanitization algorithm S, let $S(D) = D'$ be the sanitized dataset. If $\mu(P, D) > 0$, then, for S to be acceptable in the context of personalized recommendations, $\mu(P, D')$ must also be positive.

5.4.5 Measuring Privacy

Privacy-preserving data publishing work has given strong privacy foundations in sanitizing datasets, by making rows undistinguishable or protecting against attribute disclosure, while preserving some utility. Most work in this area establishes a privacy guarantee as a fixed objective and sees utility as an optimization target. However, this utility is commonly evaluated through a proxy metric instead of being measured in a personalized recommendation context. Because of this, most methods destroy utility well beyond the limit defined in Section 5.4.4. An alternative, departing from the privacy preserving data publishing tradition of a static privacy guarantee, would be considering a privacy metric and attempting to improve the overall privacy-utility trade-off in data publishing for personal recommendation scenarios.

Instead of a discrete mathematics privacy guarantee, let's consider a probabilistic model, enabling resistance to error in the adversary's auxiliary information. Also, instead of protecting absolutely against one type of attack, consider that the ultimate goal of the adversary is to enrich his knowledge on the user.

After gaining access to a database which may contain a record that refers to that user, the adversary attempts to match his auxiliary information against the records in the database. In case a record is found that sufficiently matches the auxiliary information, the adversary considers the re-identification successful. If not, the adversary considers that his attack failed, either because the user is indistinguishable or not present in the database.

The attack model used to measure privacy in this work was based on the re-identification of Narayanan and Shmatikov [2008]. The strength of this attack model is well supported in the original paper, and has been a reference for subsequent theoretical work [Merener 2012]. One of the reasons why the attack is so successful draws from the common long-tailed support distribution of sparse high-dimensional datasets: there is a small number of attributes that have non-null values for many records while there is a large number of attributes that only have non-null values for a few records. This long-tailed distribution makes records very distinguishable even by merely considering which attributes are defined and which ones aren't. This represents a privacy threat even if attribute values are obfuscated or omitted [Narayanan and Shmatikov 2008; C. C. Aggarwal 2005], rendering value obfuscation techniques almost useless since the very existence of a value is often enough to convey the information necessary for a re-identification attack.

A natural metric for studying re-identification attacks in a probabilistic setting is the success probability of the re-identification. This success probability is expected to increase with the increase in auxiliary information, so it is presented as a function of the amount of auxiliary information available to the adversary. However, this metric does not capture the information-centric notion of privacy breach described in Section 5.2.2. A trivial case where there is no privacy breach with a successful re-identification is the one in which the auxiliary information already contains all of the user's attributes that are non-null for the attacked dataset, as the adversary's knowledge on the user remains unaltered. For that reason, let us define a new privacy metric that does.

An adversary has access to an attacked dataset D, and to auxiliary information aux_x about user x - a set of ratings that user x gave to items present in D. Let I be his re-identification attack function, which outputs the set of ratings present in dataset D correctly identified to belong to user x, and an empty set otherwise. Then, let the Adversary Gain (AG) of an attack on dataset D targeting user x be:

$$AG(D, aux_x) = |I(D, aux_x)| - |I(D, aux_x) \cap aux_x|$$

A key benefit of this metric is that it allows us to take an economical look on an attacker's incentives. In a variety of scenarios, security and privacy does not need to be absolute, but instead good enough to render attacks economically unviable. If AG can be brought under certain values, this will surely be the case. Assuming the cost of performing one attack is greater than the reward of acquiring one rating, a target value of 1 for AG would be an acceptable value. However, an estimation of acceptable AG values is out of scope of this work, as it would require data on attack cost.

5.4.6 Rationale of Record Fragmentation

Most work in recommender systems attempts to identify similarities between users in order to perform recommendations. The underlying assumption is that if some users rated n items similarly, they will also rate other items similarly [Su and Khoshgoftaar 2009]. The characteristic that makes recommenders perform well are similarities between users, and it must be possible to process a dataset in a way to leverage those same similarities to make users more indistinguishable in the dataset, achieving better privacy at a very reduced utility cost.

In the context of computer communications and networks, the concept of pseudonym has been extensively used to designate a temporary or scoped identifier of a subject [Pfitzmann and Hansen 2010]. An historic reference to "digital pseudonym" is made in a 1981 paper by Chaum [1981] while describing the use of public key cryptography in such a way that it allows users to send verifiable messages while protecting their identity. Subsequently Chaum described the use of digital pseudonyms for interacting with multiple organizations while preventing that these organizations collude in order to build a profile of the user [Chaum 1985]. The pseudonym used with one organization is unlinkable with the one used with another organizations. Furthermore the user can prove the possession of some credentials obtained from one organization to another without revealing the pseudonym he uses to interact with the first. While the typical case is to use one pseudonym per organization the use of one-time pseudonyms, and more generally multiple pseudonyms per organization, is also mentioned.

In this work the concept of pseudonyms is used in the context of privacy-preserving high-dimensional data publishing. Each record - representing an individual - is split into several records with different identifiers, i.e. pseudonyms, and the values of non-null attributes are distributed among the new records, i.e. fragments. As a direct consequence the linking between different attribute values is broken. No values are changed, inserted or deleted: sets of values are simply unlinked from each other. Each

Figure 5.1: Record Fragmentation Example

(a) Original Dataset

UID	M1	M2	M3	M4	M5
1	3		5	4	
2		2	5	5	1
3	4			1	
4	3		3	2	4
5	4		5		4

(b) Fragmented Dataset

Nym	M1	M2	M3	M4	M5
1	4			1	
2	4				4
3		2			1
4	3				
5			5	5	
6			5		
7			3	2	
8	3				4
9			5	4	

(c) Pseudonym Mapping

Nym	UID
1	3
2	5
3	2
4	1
5	2
6	5
7	4
8	4
9	1

record is fragmented in several pseudonymous versions of it. The linking of these fragments using pseudonym mapping information restores the original data, thus is to remain unpublished. From a data privacy perspective, record fragmentation is vertical partitioning applied per record. Previous work has employed different forms of vertical partitioning to improve privacy, however it was either applied in the dataset as a whole [Zakerzadeh, C. Aggarwal, and Barker 2014] or to horizontal partitions of the dataset [T. Li et al. 2012; Manolis Terrovitis, Nikos Mamoulis, Liagouris, et al. 2012]. In record fragmentatio each record is an horizontal partition and vertical partitioning is applied independently to each of them. This approach also has similarities with Gkoulalas-Divanis and Loukides' clustering-based anonymization [Gkoulalas-Divanis and Loukides 2012]: these fragments are conceptually similar to their clusters, but instead of using generalization, only suitable for high-dimensional itemset datasets, dissassociation is used.

Record fragmentation is illustrated in Figure 5.1: each record of the original dataset is split in several, forming the sanitized dataset and the mapping between the identifiers of the two datasets. Let's assume that the sanitized dataset is accessible to the adversary while the mapping dataset is either destroyed, stored securely, or distributed among the users - each user holds the pseudonyms that refer to him.

The choice of which values are presented together and which are separated in different fragments is done based on the statistical properties of the dataset. Following the principles used in condensation approaches [C. C. Aggarwal and Yu 2004], it is desirable to keep inter-attribute correlations as much as possible in order to reduce the utility loss. In order to do so, a meaningful distance measure between dataset values is required. However, it has been argued that the distances to the nearest and farthest neighbours from a given target in high-dimensional space is almost the same for a variety of data distributions and distance functions [C. C. Aggarwal 2005; C. C. Aggarwal, Hinneburg, and Keim 2001; Beyer et al. 1999]. For that reason some dimensionality reduction technique should be applied before using distance functions. Also, records with greater support can be fragmented more times than records with smaller support, in order to avoid the *new user* problem of recommender systems as much as possible.

On the privacy side, the aim is to reduce the amount of information conveyed by the presence of a (non-null) value. The amount of information is directly related to the frequency of the value: if only a few records have a value assigned for a specific attribute, then that attribute is more distinctive than others. Separating rare occurrences of values is key to make records less distinguishable, increasing resilience to re-identification attacks [Merener 2012].

5.4.7 Record Fragmentation Algorithm

In order to formally describe the algorithm, the matrix model of datasets is used. Let dataset D be an N x M matrix where each row r_i is associated with an individual and each column c_j with an attribute. Record $d_{i,j}$ refers to the value that the individual associated with r_i has for the attribute associated with column c_j.

In order to estimate column distance, so that the fragmentation can be done minimizing the error, matrix factorization was used as a dimensionality reduction technique. In a preprocessing step D is factorized in f features, originating two matrices: the RF N x f matrix, showing the correlation between rows and features, and the CF f x M matrix, with the correlation between features and columns. Also during preprocessing, the support - the number of non-null values of each row or column - is respectively captured in vectors RS and CS. The algorithm then generates the dataset D', an P x M matrix, in which P is the total number of pseudonyms used, greater than N, the original number of individuals. Each row of D' is basically a fragment of an original row r_i of D.

To perform the fragmentation, values are clustered together based on their column characteristics. A number of the lowest support columns for which an original row has values defined are fixed as centroids for each new record. The number of lowest-support columns that are elected as centroids depends on the chosen privacy-utility trade-off parameters. After the centroids are assigned, a simple one-pass value assignment is performed based on a distance measure between the column of the value and the defined centroids. This is a lightweight approach to grouping allowing column-neighbour values to be kept together, especially when compared with possible alternatives which include clustering algorithms like K-Means.

The algorithm starts by iterating over the N rows r_i of D, each generating a number of new rows in D'. Given an original row r_i, the collection of j for which $d_{i,j}$ is non-null is temporarily stored and sorted in ascending order by their cardinality value cs_j. The resulting vector J is used to create the new rows iteratively. In case the cardinality value cs_j of the current iteration is below a certain threshold t, then a new row d'_p is created in D', otherwise the row creation iterations for that original row r_i stops.

Let X be the number of successful iterations, and consequently the number of assigned pseudonyms for original row r_i. For each r_i a X x f temporary centroid matrix CFi is built by assigning the column features cf_j for the X first values of J. Finally the algorithm iterates over the records $d_{i,j}$ of row r_i, assigning each of them to one of the new rows d'_p. For that the feature vector cf_j is considered and its distance is calculated to each of the rows in CFi, which represent the centroids. The record is assigned to the centroid to which it has lowest distance and assigned to the corresponding new row.

Algorithm 1 Pseudonymization Algorithm

```
initialize $D'$;
for all $r_i$ do
    initialize $CFi$;
    $x = 0$;
    for all $cs_j$ referring to $d_{i,j}$ in $r_i$, by ascending order of values do
        if $cs_j \leq t$ then
            add row $d'_p$ associtated with $x$;
            add row $CFi_x$ with the values $cs_j$;
            increment $x$
        else
            break;
        end if
    end for
    for all $d_{i,j}$ in $r_i$ do
        for all $x$ in $CFi_x$ do
            $temp_x = dist(j, CFi_x)$
        end for
        $x_{min} = x$ for the value of $x$ that minimizes $temp_x$
        add record $d_{i,j}$ to row $d'_p$ associated with $x_{min}$;
    end for
end for
randomize row order of $D'$;
```

The result of the algorithm is dataset D', an P x M matrix such that P $\geq$ N, and that has the same number of non-null records as D. The distance function *dist* used in the conducted experiments was Euclidean Distance but other distance measures could be considered. Experimenting with different distance measures would likely slightly influence the RMSE, but the results obtained with Euclidean Distance were enough to demonstrate the potential of this approach, as shown by the results in Section 5.5. Instead, it was decided to experiment with different thresholds t, because this parameter has a key influence in the privacy-utility trade-off.

A function was used to calculate the threshold value t in each iteration, instead of a fixed value. This allows us to tune the amount of created fragments per row. The considered threshold function takes in 2 parameters. The first is an estimation for a threshold attribute cardinality value, tc, indicating whether a non-null value is considered a rare occurrence. The second is a target number of fragments for a user, np, depending on the cardinality of that user. The function itself is linear: the threshold value is the estimated attribute cardinality when the number of attributed pseudonyms matches the target number of fragments, and it varies with the number of attributed pseudonyms, x.

$Thr(tc, np, x) = tc * (x/np)$

The second parameter is itself also a function that maps user cardinality to the target number of fragments. For this end, a logarithm-based function was used, which can be parametrized in order to allow increasing or reducing the target number of fragments for the same user cardinality, $|u|$, respectively leading to more privacy or more utility. Logarithmic was picked over linear because it preserves the long-tail of the user cardinality frequency function, which is characteristic for this kind of datasets, otherwise the application of the algorithm would be trivial to detect. The two parameters, *logp* and *linp*, allow varying the $NPseudo$ function both linear and logarithmically.

$$NPseudo(logp, linp, |u|) = linp * log(1 + (|u|/logp))$$

The impact of parameter variation in pseudonym attribution is empirically analysed in section 5.5.7.

5.5 Record Fragmentation: Experiments and Results

5.5.1 Netflix Prize Dataset

During the duration of the Netflix Prize contest anyone could download the Netflix Prize dataset and tools, write their movie recommendation algorithm, test the results locally with a probe set and submit the results for the qualifying set. The prize was awarded to the algorithm that produced the predictions with the lowest Root-mean-square error (RMSE) for the qualifying set. The baseline for the contest was Netflix's original algorithm, Cinematch, which scored 0.9514 RMSE, and the objective was to improve that result by 10%. The Grand Prize was won by an aggregate team of previously competing teams called BellKor's Pragmatic Chaos [Netflix 2009]. Their algorithm scored 0.8567 RMSE, a 10.06% improvement on Cinematch.

The dataset consists of movie ratings, from 1 to 5, submitted by Netflix users, with the submission date, organized by movie id. The movie ids are sequential and range from 1 to 17770, unlike user ids, which range from 1 to 2649429 but amount to only 480189 distinct values. The dataset accounts for a total of 100480507 ratings, which represents 1.1% of the possible rankings for the considered number of users and movies.

5.5.2 Movielens Dataset

In order to compare the results in different datasets, another freely available well-known movie ratings dataset was considered. Movielens is a dataset made available by the University of Minnesota, crowdsourced via their web site [GroupLens 1997], with the purpose of gathering data for research in recommendation systems and providing movie recommendations to users. There are currently three releases of the dataset made available to the public [GroupLens 2011] which have different sizes with the biggest having 10000054 ratings - significantly smaller than the 100 million ratings from Netflix. These ratings are given by 69878 users to 10677 movies, which means Movielens is slightly less sparse than Netflix having 1.3% non-null values.

For the experiments described, the Movielens dataset was converted to the Netflix format, so that the same setup and code could be used. This included rounding the ratings up because Netflix supports integer ratings from 1 to 5 while Movielens supports 10 possible values for ratings: 0.5 to 5 with 0.5 steps. Because the goal is simply to compare the recommendation accuracy between the original and resulting datasets, the pre-experiment rounding process isn't an influencing factor.

5.5.3 Reference Re-Identification Algorithm

Narayanan and Shmatikov presented a generic algorithm for re-identification in sparse datasets and applied it to the Netflix dataset with interesting results [Narayanan and Shmatikov 2008]. The algorithm has two variations named Scoreboard and Scoreboard-RH, and they both rely in the overwhelmingly low similarity between users of the dataset. The mere information about which movies users rated makes them very distinguishable, especially because of non-mainstream movies which are not rated by many users. Even with incorrect and incomplete auxiliary data or dataset perturbation, it is possible to re-identify many users with a good probability. Narayanan and Shmatikov defined similarity between two rows as a kind of cosine similarity. *Sim* maps a pair of records to the interval [0,1] according to their similarity. The Scoreboard-RH algorithm is a more robust version than Scoreboard and it defines a scoring function *Score* which assigns a numerical score to each record in the database D based on how well it matches the attacker's auxiliary information *aux* about an individual.

$$Score(aux, d_i) = \sum_{j \in supp(aux)} wt(j) \times Sim(aux_j, d_{i,j}) \text{ where } wt(j) = \frac{1}{\log |supp(j)|}$$

After *Score* is calculated for all the rows d_i Scoreboard-RH takes the two highest scores and calculates how different they are in relation to the standard deviation. If the value is bigger than a defined "eccentricity" parameter ϕ, then the best match is considered to be a successful re-identification. Otherwise the algorithm outputs no match.

$$\frac{max1 - max2}{\sigma} > \phi$$

In order to evaluate how susceptible the resulting datasets are to re-identification, Scoreboard-RH was implemented. Original work considered that *Sim* would output 1 on a pair of movies rated by different subscribers if the ratings and dates are within some threshold, and 0 otherwise. For simplicity purposes, and to consider the same data in the utility and privacy analyses, dates are disregardede in this implementation of Scoreboard-RH, relying only on the ratings information. Apart from that, this version of Scoreboard-RH was instantiated similarly to the one of Narayanan and Shmatikov:

- the *Sim* function will output 1 in case the rating of a movie in the two rows matches and 0 otherwise;
- the eccentricity parameter ϕ is set to 1.5.

Re-identification is successful in case the algorithm outputs any pseudonym that refers to the user to which the supplied auxiliary information belongs to. This Scoreboard-RH implementation uses a random sampling approach to evaluate the re-identification success: auxiliary information of a certain size referring to a random individual from the original data set is randomly sampled and used to match it in a target dataset. The estimation of the results is done for a 95% confidence interval and 2% error margin, so the sampling is repeated according to the number of samples required using the normal approximation for a binomial proportion interval (Wald interval). This meant 300 iterations in the best case and above 2400 in the worst case.

5.5.4 Reference Recommendation Algorithm

Motivated by the Netflix Prize competition, there was source code contributed by contestants that could be used to perform basic operations with the dataset. Two contributions deserved attention: the Netflix Recommender Framework [Meyer 2006] and, based on it, the Kadri Framework [Kadri 2008]. These frameworks provide functions to efficiently process the Netflix dataset text files, as well as implementations of some recommendation algorithm primitives, namely average, matrix factorization, K-NN and prediction blending. Another function provided by these frameworks is the possibility to scrub the probe data from the dataset: the probe data is removed from the training set, effectively separating the training and test sets, increasing the reliability of the RMSE results.

Using these frameworks, a reference prediction algorithm was created by blending movie average and matrix factorization predictions. These algorithms ignore date information, relying only on movie ratings, similarly to what was done regarding the re-identification algorithm, described in Section 5.5.3. This reference prediction algorithm scored 0.921299 RMSE on Netflix, a better result than the original Cinematch algorithm.

5.5.5 Reference Privacy Preservation Algorithm

From all the identified previous work, the one most similar to record fragmentation is disassociation [Manolis Terrovitis, Nikos Mamoulis, Liagouris, et al. 2012]. As explained in Section 5.4.6, both methods use forms of horizontal and vertical partitioning to fulfil their objective of protecting privacy in high-dimensional datasets. The main difference is that disassociation has k^m-anonymity as its objective, a static privacy guarantee, while record fragmentation has a target number of fragments function, representing the privacy-utility trade-off.

Disassociation was chosen also because k^m-anonymity is one of the most relaxed privacy guarantees defined, and yet not relaxed enough to cope with personal recommendation scenarios. The partitioning applied with disassociation generates a dataset where the great majority of records have a support of 1 or 2, as explained in the choice of the evaluation parameters [Manolis Terrovitis, Nikos Mamoulis, Liagouris, et al. 2012, p. 952]. This may be enough for associating query some items together but not to perform personalized recommendations. In order to validate this concern, the disassociation algorithms, VerPart and HorPart [Manolis Terrovitis, Nikos Mamoulis, Liagouris, et al. 2012], were implemented targeted at achieving the most relaxed privacy guarantee possible with that method: 2^2-anonymity. Because m was set to 2, it wasn't necessary to implement the Refine algorithm, as it only has an impact for $m > 2$.

5.5.6 Implementation Detail

One of the issues of processing the Netflix dataset is technical: it's not easy to load such an amount of data in a quick and memory-efficient manner. For that reason a Netfix Commons library was created in Java to solve that problem, loading the dataset to memory and providing an API to access the data. Heuristics were used to improve access times to data without requiring more memory for the representation. Both Scoreboard-RH and Record Fragmentation implementations created for this work use this library.

The preprocessing and main steps of the algorithm described in Section 5.4.7 were implemented separately. The preprocessing step that involves matrix factorization and attribute cardinality count, which in the Netflix case is the number of ratings per user,

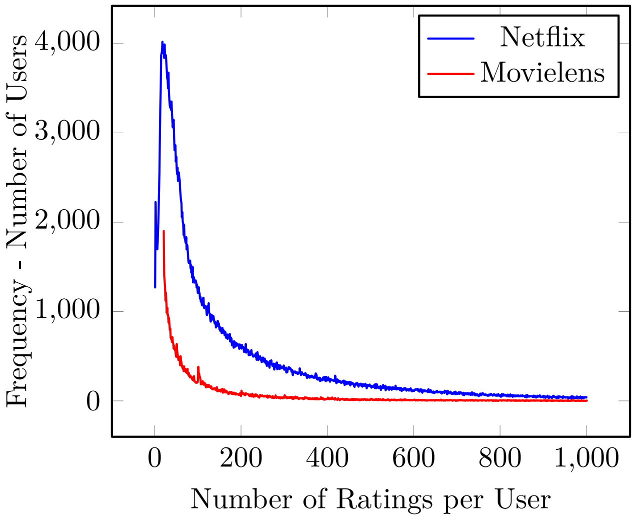

Figure 5.2: Frequency of the Number of Ratings per User for Users with Under 1000 Ratings

was implemented in C++ using the Kadri Framework. This generates 3 text files each containing a matrix: user-features, movie-features and user ratings. The main step of the algorithm was implemented in Java. It requires access to the 3 text files from preprocessing and to the original data set, and it generates the fragmented version of the dataset in the same format as the original one, a probe file in accordance to the resulting dataset, and a pseudonym mapping file to match the attributed pseudonyms to the original user ids for evaluation purposes. For performance purposes, a safe cardinality value for movies was introduced in the implementation. If the movie has a number of ratings above this value then it is not considered to be a centroid. This significantly reduces the number of movies that must be sorted by cardinality, consequently reducing the time that quicksort takes.

5.5.7 Dataset and Partitioning Analysis

Support analysis to both datasets shows similar long tail patterns both regarding users and movies: a few movies/users have many (non-null) ratings while the majority of users/movies have only a few ratings, as shown in Figures 5.2 and 5.3. Netflix shows frequency maxima in users and movies for low cardinalities: 18 and 119 respectively. Movielens has their maximum frequency values for the lowest cardinalities possible: 20 for users and 1 for movies - the Movielens site imposes that each user rates at least 20 movies on registration so that it can deliver meaningful recommendations, avoiding the *new user* problem.

The algorithm preprocessing step described in 5.4.7 was run only once on each of the original datasets to create the required matrix files. Then the main algorithm was run several times, each of the runs generating a fragmented version of the original dataset. Different privacy-utility trade-off parameters were used in each run, resulting in different fragmentation levels. As described in Section 5.4.7, the considered trade-off parameters were:

- the movie cardinality safe value, until which movies are considered to initialize group centroids;

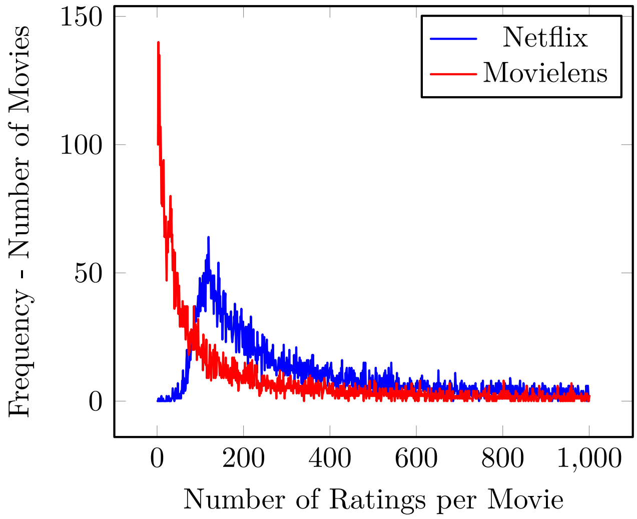

Figure 5.3: Frequency of the Number of Ratings per Movie for Movies with Under 1000 Ratings

- the target movie cardinality value, the last value for which a movie is elected as a centroid in case the user was assigned exactly the target number of pseudonyms;
- the target number of fragments function, for which were assumed different parameters for the logarithm function.

The first two parameters were set based on the movie cardinality of the dataset, as shown in Figure 5.3. The movie cardinality safe was set to a conservative value of 5000, merely for improving the algorithm processing times, expected not to influence the number of created fragments. The target movie cardinality value was set to 500 by looking at the Netflix movie cardinality distribution, as it represents the start of the long tail and divides the movie domain in half: approximately 48% of the movies have less than 500 ratings. In order to simplify, since both an increase in the target movie cardinality and a linear increase on the target fragments is equivalent, let's consider these first two parameters to be fixed and vary the target number of fragments function for the trade-off.

The fragmentation experiments were run on a virtual machine with 1 virtual core and 4GB of RAM allocated, running Java HotSpot VM on Ubuntu Linux, hosted by a Intel Core i7 machine. The measured run-times for the Netflix dataset were approximately 10 minutes for the least aggressive fragmentation and 1 hour for the most aggressive one. For the Movielens dataset the run-times were from 2 to 11 minutes. These results confirm the expected linear run-time scalability with respect to the target number of fragments, as well as an overhead related to the size of the dataset for input/output operations. In the same conditions, the implementation of 2^2-anonymous disassociation took orders of magnitude longer to be completed: approximately 9 hours for Movielens and 95 hours for Netflix. Note that these results suggest that the algorithm run-time grows linearly with the number of ratings, as Netflix has approximately 10 times more ratings than Movielens, but conclusive results would require further work.

The target number of fragments function, as described in Section 5.4.7 is based on a logarithm function to which two parameters are applied, one allowing to vary the

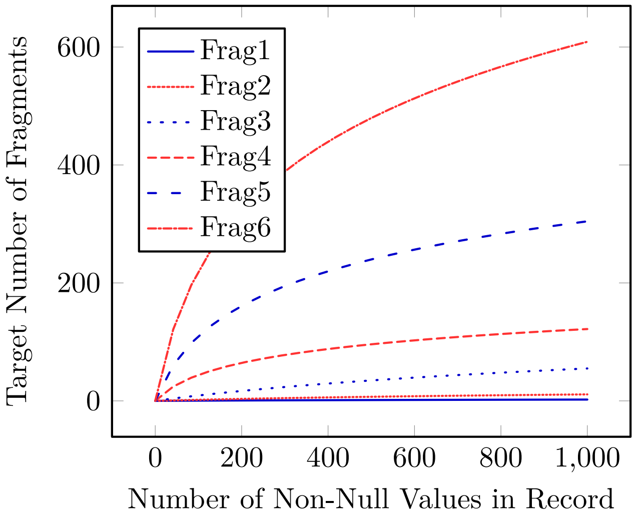

Figure 5.4: Functions for Target Number of Fragments

Table 5.2: Number of Rows in the Original and Fragmented Datasets

Dataset	Netflix	Movielens
Original	480189	69878
Frag1	746153	157421
Frag2	1441715	330961
Frag3	3057962	735668
Frag4	5039491	1324378
Frag5	7292946	2008289
Frag6	9111456	2676293
2Dis	82685159	8437233

function linearly and other logarithmically. The tested functions, numbered from 1 to 6 based on how they affect the privacy-utility trade-off, are depicted in Figure 5.4, being 1 the most utility-friendly and 6 the most privacy friendly. The fragmented datasets resulting from applying the algorithm with each of these functions are named based on the function numbering. Table 5.2 shows the number of rows of the resulting datasets that differ based on the used function parameters, both for the Netflix and Movielens cases, compared with the number of rows resulting from 2^2-anonymous Disassociation. As expected (see Section 5.5.5) the number of rows generated by 2^2-anonymous disassociation comes very close to the number of total ratings. The average row support of 2^2disassociated Netflix is 1.215, and for Movielens is 1.185, illustrating the strictness of the method.

5.5.8 Utility Evaluation

In order to evaluate the results in terms of utility, the recommendation algorithm implementation described in Section 5.5.4 was run in the original and fragmented datasets. As discussed in Section 5.4.4, the RMSE value itself does not convey a direct understanding on the utility loss in the context of personalized recommendations. For that reason the Personalization Utility (μ) metric is used. In order to calculate it, the average movie rating was considered the naïve prediction function, thus the following RMSE

Table 5.3: RMSE of the Predictions for the Different Datasets

	Netflix		Movielens	
Dataset	RMSE	μ	RMSE	μ
Average	1.05282	0	0.946021	0
Original	0.921299	0.124923	0.874797	0.075288
Frag1	0.931068	0.115643	0.855595	0.095585
Frag2	0.944055	0.103308	0.850197	0.101292
Frag3	0.978027	0.071041	0.852461	0.098899
Frag4	0.979276	0.069854	0.862424	0.088368
Frag5	0.981908	0.067355	0.869907	0.080458
Frag6	0.985127	0.064297	0.875914	0.074108
2Dis	1.053909	-0.001034	0.948689	-0.00282

values as reference: 1.05282 for Netflix and 0.946021 for Movielens. These RMSE values of the naïve prediction are the same for all datasets because both record fragmentation and Terrovitis' Disassociation both rely exclusively on partitioning, leaving the ratings themselves and their association to movies unaltered.

The RMSE results, as well as the utility metric μ, are depicted in Table 5.3. It can be seen that, generally, the higher the fragmentation, the more significant is the utility loss. However this is not true for the more utility-friendly Movielens generated datasets, where a RMSE reduction is observed. This is explained by a side-effect of the algorithm and chosen metrics. Similarly to what is observed for the condensation method, where the classification accuracy improves due to a noise reduction effect [C. C. Aggarwal and Yu 2004], in the fragmentation case keeping nearest movies together initially increases prediction accuracy. The minimum error is reached at certain fragmentation level, where the information being removed from the dataset is no longer mostly noise and starts to be useful information, observed to be close the average of 5 fragments per record. After that point the utility-improvement effect fades as the fragmentation becomes more aggressive, exhibiting degraded utility at the most fragmented case tested. Disassociation, because it strictly enforces a privacy guarantee, even its most relaxed instantiation, 2^2-anonymity completely destroys μ. Otherwise successful prediction algorithms become less useful, when applied to a disassociated dataset, than considering the movie average for prediction.

5.5.9 Re-Identification Evaluation

To evaluate the risk of re-identification, Scoreboard-RH was run using the implementation described in Section 5.5.3, with the auxiliary information being built randomly from the original dataset. This enables the evaluation of re-identification success with increasing sizes of auxiliary information, at the cost of some generality: for higher values of auxiliary information the random sampling becomes skewed as not all users can be considered, only the ones that have at least the required number of ratings.

The re-identification success of the fragmented datasets behaves similarly as it does on the original dataset, as seen in Figure 5.5: re-identification success rises rapidly as available auxiliary information size increases. The re-identification success reaches a limit for auxiliary information sizes of 20 to 25 for all the versions of the Netflix dataset.

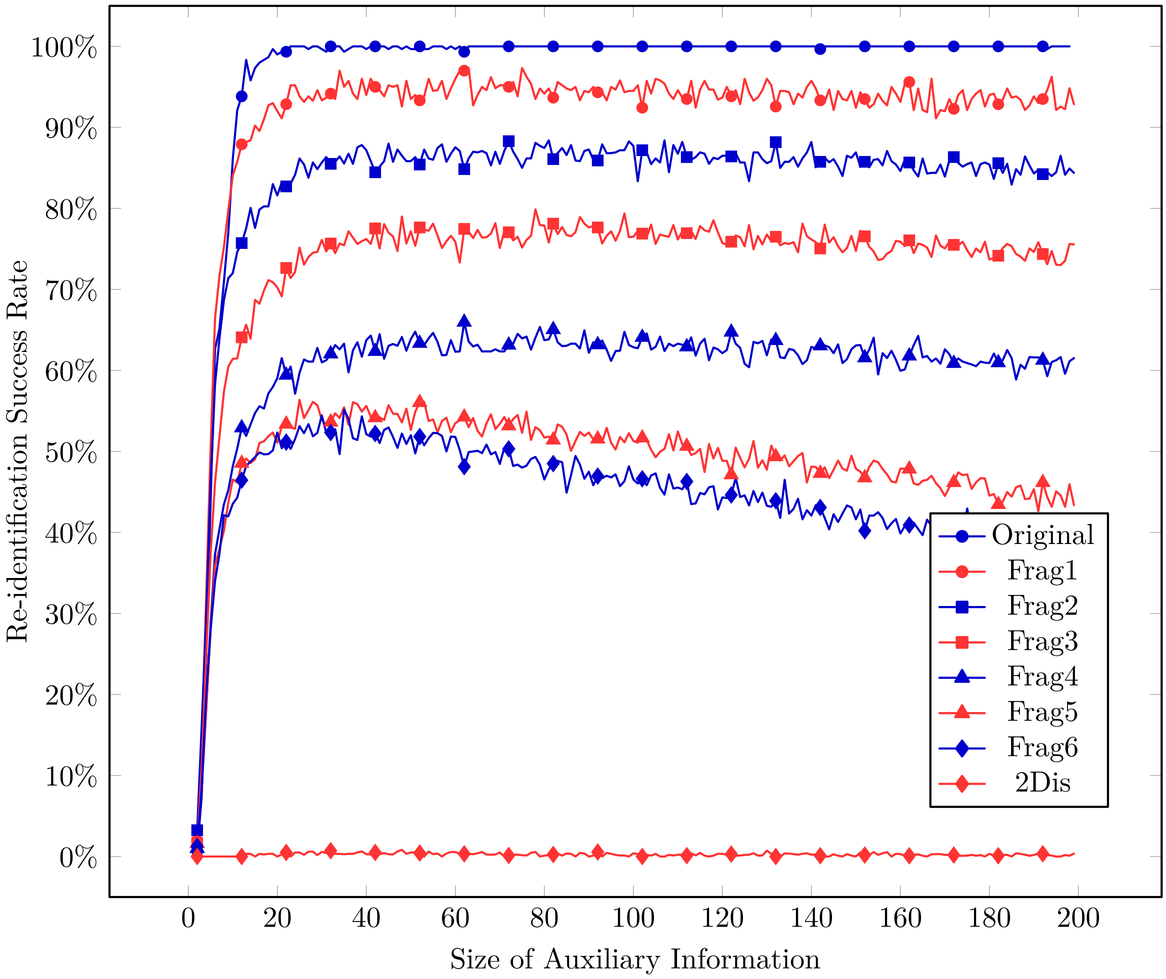

Figure 5.5: Re-identification Success Rate on Original and Generated Netflix Datasets by Size of Available Auxiliary Information

The difference is the limit value: while for the original dataset the success rate reaches 100%, as previously shown by Narayanan and Shmatikov, for the fragmented ones the limit is lower, proportionally to how aggressive fragmentation was.

Similar behaviour is observed for the original Movielens dataset (Figure 5.6), with Scoreboard-RH reaching 100% re-identification success for the same values of auxiliary information size. The fragmented datasets also exhibit comparable behaviour with increases in re-identification success for increasing size of auxiliary information until the limit is reached at approximately the same values. However in this case, as fragmentation increases, the "limit" clearly becomes a decreasing function: more auxiliary information apparently leads to less re-identification success. This is originated by the skew effect previously referred: auxiliary information generation is more skewed towards users with more ratings for higher sizes. The decrease of re-identification success with the increase of auxiliary information size merely shows that users that originally had more ratings are better protected against re-identification. Although this can be observed more clearly in Movielens fragmented datasets, it is also noticeable in Netflix's most aggressively fragmented datasets.

Because 2^2-anonymity only guarantees protection against an adversary with knowl-

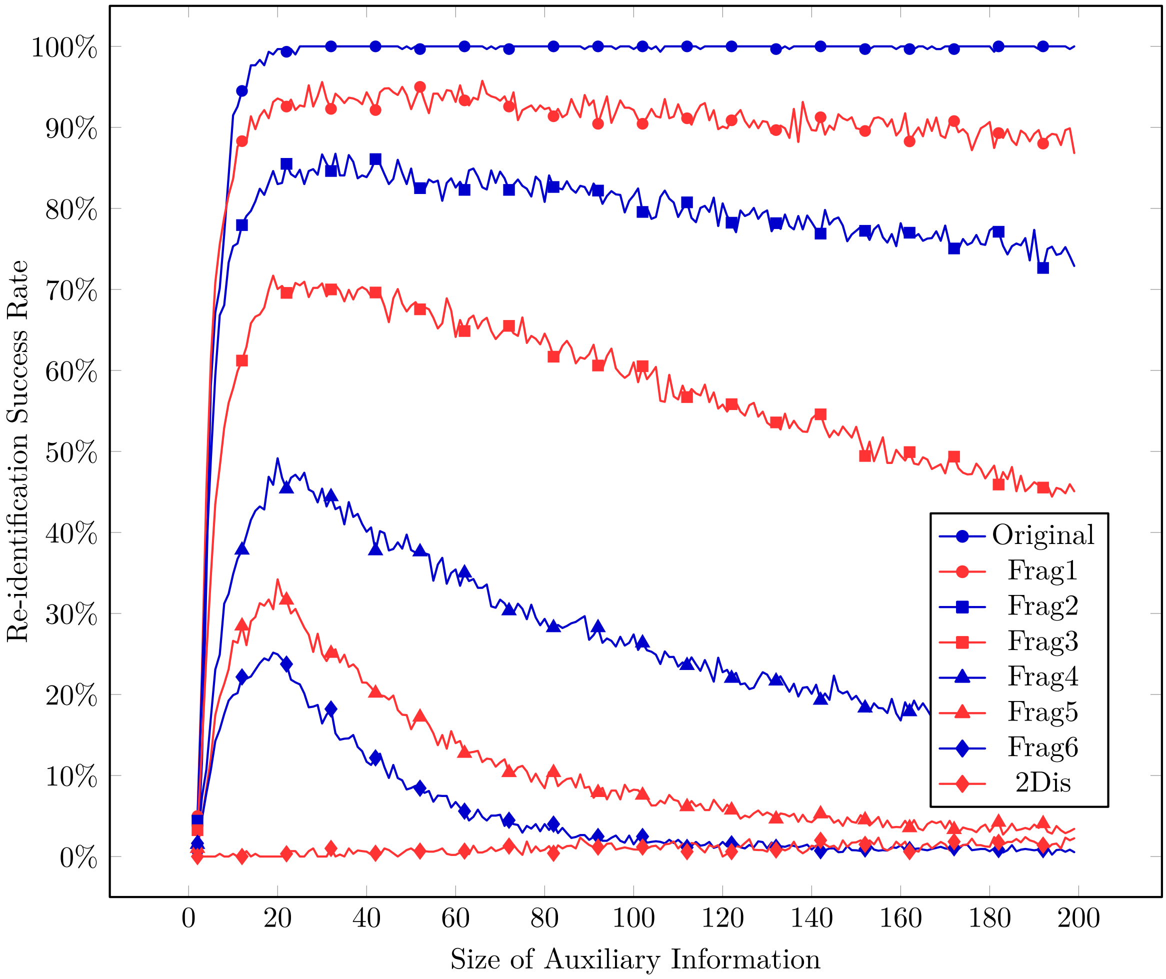

Figure 5.6: Re-identification Success Rate on Original and Generated Movielens Datasets by Size of Available Auxiliary Information

edge of at most 2 items, as the auxiliary information size increases the probability of it containing more than 2 non-disassociated items also increases. Consequently, the 2^2-disassociated dataset behaves in an inverse manner to the fragmented ones, with re-identification probability steadily rising with increases in auxiliary information, but at very low values.

Because of the auxiliary information sampling skew effect, the re-identification success limit was considered to be the average of the auxiliary information size saturation region, where global maxima are found for most aggressively fragmented datasets. In Figure 5.7 the limit values of re-identification results - success, inconclusive or wrong result - for each of the datasets are shown. Inconclusive results grow faster for low fragmentation datasets and then stabilize around 30%. Scoreboard-RH shows significant resilience to wrong results for low fragmentation datasets, but as fragmentation increases wrong outputs become more noticeable, especially after inconclusive results stabilize. Netflix and Movielens datasets show similar behaviour, with the Movielens dataset showing itself as more privacy-friendly than Netflix.

Unsurprisingly, 2^2-disassociation is extremely effective against Scoreboard-RH, returning an inconclusive result around 95% of the times for both datasets. However,

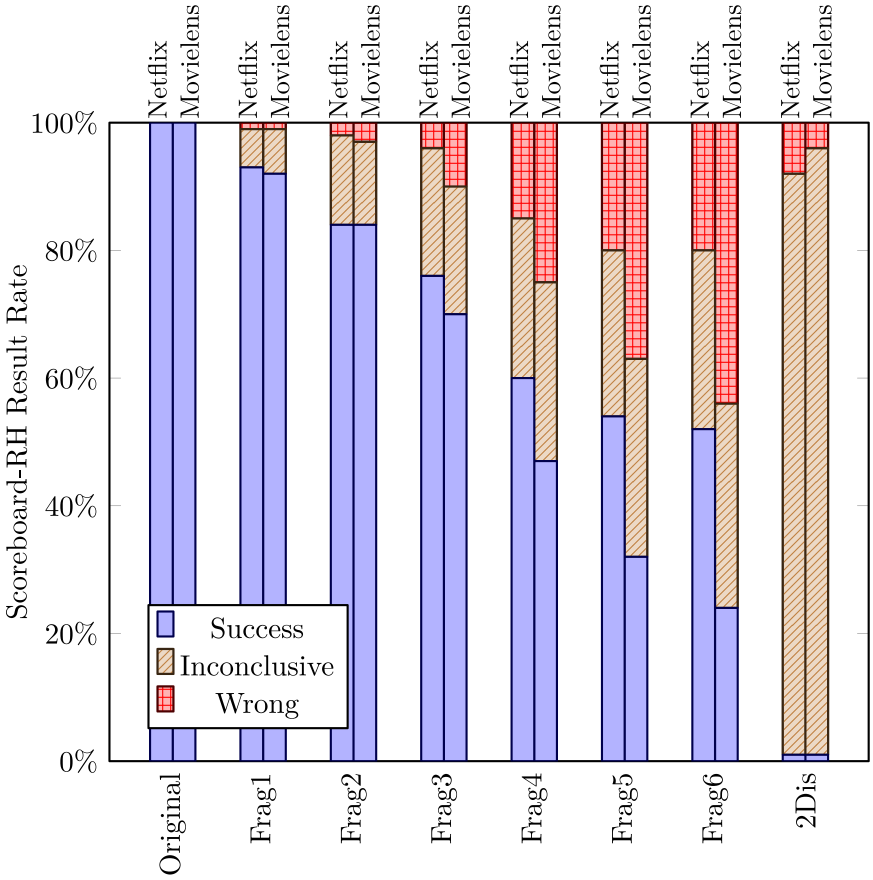

Figure 5.7: Scoreboard-RH Limit Results per Dataset

Scoreboard-RH does manage to successfully re-identify the target in a few occurrences, demonstrating its strength. Furthermore, in real-life scenarios it may be beneficial that the adversary isn't able to trivially detect the use of a sanitization algorithm. While *AG* shows no difference between wrong and inconclusive results, from an economical point of view it's worse for an adversary to have false positives (wrong results) than true negatives (inconclusive results) [Herley 2012].

5.5.10 Adversary Gain Evaluation

As argued in Section 5.4.5, because re-identification rate is an incomplete privacy metric, the *AG* metric was also calculated. This metric estimates the worth of the attack from the adversary's point of view - higher values mean less privacy. The goal of a sanitization algorithm doesn't have to be no *AG*, but a low enough value that makes attacks economically unviable.

Figure 5.8 shows the *AG* significantly decreases for fragmented datasets, especially for the Movielens case. Generally, relative to the original case, the reduction in *AG* is significantly greater than the reduction of μ for the user. This indicates that record fragmentation has a positive effect on the overall privacy-utility trade-off. 2^2-disassociation renders an absolutely residual *AG*, as positive *AG* can only occur for successful re-identification of rows with more than 2 items, which comprise of a very small fraction of the disassociated dataset.

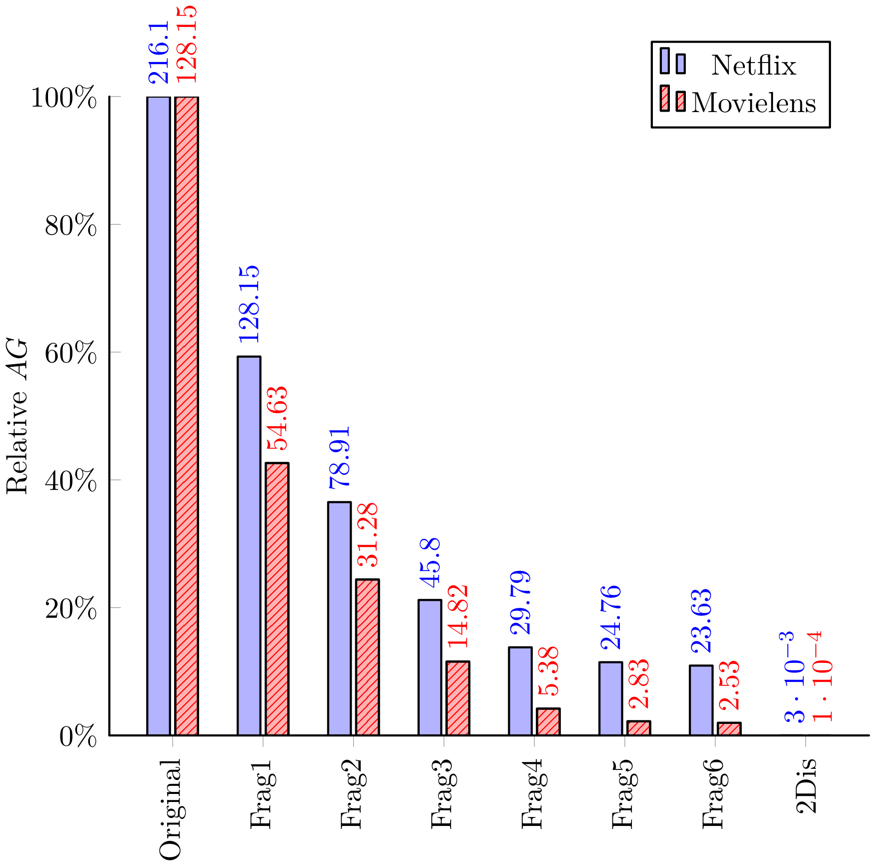

Figure 5.8: Average Limit *AG* per Dataset

5.6 Conclusions

The fields of PPDM and SDC enable benefits of data mining and statistics while preserving the privacy of individuals whose data is part of the analysed datasets. Work such as k-Anonymity [Sweeney 2002] and t-Closeness [N. Li, T. Li, and Venkatasubramanian 2007] have addressed privacy for databases that contain sensitive information as well as and other information that can be used to re-identify the user. They focus in privacy guarantees that stop attackers with auxiliary information to retrieve sensitive information about users. Another approach is the one of Differential Privacy [Dwork 2006] which lays out a strong mathematical foundation for subsequent data-privacy work [Dwork 2008].

However, existing work in privacy preserving data publishing for the high-dimensional case is currently not useful for recommendation scenarios. The proposed privacy guarantees destroy the benefits that can be harnessed by publishing datasets, because similar recommendations are possible by simply accessing aggregate data. However, the user patterns that make personalized recommendations possible may also provide some degree of privacy protection to those users. Driven by this idea, a new utility metric is presented, to be used in personalized recommendation scenarios, as well as a privacy metric, to take the place of a static guarantee. An anonymization method that relies on per-record vertical partitioning is also described, inspired by distributed systems work in pseudonyms, that aims to validate that is possible to significantly improve privacy while maintaining personalization capabilities.

Personalized recommendations rely on predicting unknown ratings in a dataset, using data mining algorithms. Personalization Utility measures how well a database-algorithm pair adapts to the preferences of individual users. It's possible to evaluate loss in Personalization Utility introduced by different sanitization methods, by choosing a reference prediction algorithm and running sanitized datasets against that algorithm. The benefit of this metric is that it enables saying whether a sanitization method is applicable to personalized recommendation scenarios or not. Since personalized recommendations are a key application of data publishing, this should be a relevant contribution.

Static privacy guarantees are useful to work with, but ignore the economical aspects of security related topics. It is beneficial to measure privacy instead of *guarantee* it for two key reasons: 1) for some scenarios the utility cost of *guaranteeing* privacy is simply too high to be applicable; 2) for some scenarios it may be enough to improve privacy just to the point that it becomes economically unviable to attack it. Personalized recommendation scenarios are an example of such cases: current privacy guarantees render entire datasets as useful as aggregate data and the disclosure of a few movie ratings is not critical. In order to fill this gap Adversary Gain is proposed, which, based on some reference re-identification attack, quantifies the adversary reward: in average, how many new attributes will an attack render.

The presented sanitization method limits the probability of re-identification attack success independently of the available auxiliary information size. The method performs well regarding both metrics, reducing very significantly Adversary Gain at a reduced Personalization Utility cost. The method is completely truthful: all values are unchanged (no generalization or noise), there are no artificial values included in the result (no synthetic data), and no original value is omitted (no suppression). Instead it unlinks sets of values that belong to the same record, fragmenting them into several records based on simple metrics of privacy and utility optimization: separation of rare occurrences and link preservation of "neighbour" attributes, based on some distance function. While similar fragmentation methods are employed in related work, some methods rely in the quasi-identifier assumption [Ghinita, Tao, and Kalnis 2008; T. Li et al. 2012], and the others aim to achieve privacy guarantees that are too destructive for personalized recommendations [R. Chen et al. 2011; Manolis Terrovitis, Nikos Mamoulis, and Kalnis 2008; Manolis Terrovitis, Nikos Mamoulis, Liagouris, et al. 2012; Zakerzadeh, C. Aggarwal, and Barker 2014].

With this exercise the information-space between personalization and identification was explored, using an approach inspired in communications privacy work on pseudonyms. It is shown that, using this method, privacy can be improved while providing personalized recommendation services. The database is sanitized it in a way that greatly reduces adversary benefit, discouraging attacks. The pseudonym mapping which results from the process can be destroyed or stored in a secure, inaccessible location, because it isn't required to perform recommendations. It can also be distributed among the users' recommendation clients, enabling the combination of several estimations belonging to pseudonyms of the same user locally. Directions for future work include the development of an interactive version of the algorithm, enabling new ratings to be added to a sanitized dataset.

Chapter Six

Real Privacy for a Real World

Privacy-enhancing technologies must attend to the particularities and dilemmas of the real-world. In a world where privacy itself is undergoing discussion and transformation, it becomes of key importance to identify the issues and forces at play in this process so that future privacy challenges are catered for. Technological development will both influence and be influenced by these forces.

6.1 Introduction

6.1.1 Privacy Crossroads

Privacy is currently being addressed in a number of distinct contexts. The data handling practices of enterprises are currently being limited in the EU [Reding 2012], the surveillance practices of intelligence agencies are being questioned [Macaskill and Dance 2013], the US Congress has recently shown reserves regarding potential privacy issues raised by announced Google technology [Barton et al. 2013], and privacy impacts from the generalized use of social networks have been discussed [Hampton et al. 2011]. As the discussion of these issues progresses, the very concept of privacy is being adapted to the current times.

In order to propose privacy solutions in future scenarios it is useful analyse the current privacy dilemmas that society is facing. The nature and implications of each of these privacy-related discussions are very different. However, they are all related to technology, and become inter-related from a technological point of view. A decision of technological nature or impact aimed to address a privacy issue may influence the outcome of the privacy discussion in other contexts in unclear ways. Technology, through different bodies of knowledge, is at the centre, inter-connecting all these issues.

6.1.2 Chapter Outline

In this Chapter a multi-disciplinary analysis was conducted on the most relevant privacy issues. The different issues were analysed in their context of interest, enabling to better understand how they relate to each other and how they will shape future privacy. The macro-disciplines considered for analysis were economics (Section 6.2), law (Section 6.3) and social sciences (Section 6.4). Technological development will both influence and be influenced by these fields. Within technology, different fields will also influence and be influenced by each other, and thus a holistic view of privacy in technology is drawn in Section 6.5.

6.2 Economics of Privacy

6.2.1 An Economic Cause to Privacy Issues

In Section 2.3 a significant number of PETs are mentioned, in order to illustrate the different fields of work related to privacy. Furthermore, in Chapters 3 and 5 some of these fields are further explored, presenting ways to preserve or improve privacy guarantees in different situations. However, only a few work tracks address one of the current key types of privacy issues, as identified in Sections 2.1.4 and 6.4.1: the use of personal data for economic benefit.

The direct correspondence between data gathering and revenue has fuelled web-based companies for the last decade. In 2012 Google declared 43686 million US dollars of advertising revenue, representing 95% of total revenue [Google Inc. 2013a]. In its turn, Facebook declared 4279 million dollars of advertising revenue, amounting to 84% of total revenue [Facebook Inc. 2013]. This clearly illustrates the importance of targeted advertising in major web companies' business model.

A darker side of the personal data business is conducted by *data brokers* such as Axciom, Experian and Alliance Data. Axciom, the biggest of these companies, aggregates consumer data from multiple sources (e.g. public data available electronically, online service registration, questionnaires, magazine subscriptions, ...) and stores it in a consumer database that has approximately 1500 facts about 500 million people worldwide [Mason 2009]. The facts include:

1. contact information - name, postal address, email and phone number;
2. demographic and socio-economic data - age, income, marital status, children, education, net worth, occupation, ...
3. property data - home ownership, length of residence, home value, purchase amount and date, likely equity;
4. lifestyle - self-reported hobbies, interests and activities;
5. purchase activities - travels booked online, ...

This data is then used in order to better target advertisement, to the right customers, using the right marketing channel at the right timing, increasing its return on investment [Suther 2009].

Beyond helping companies target better their marketing investment, data brokers are also reported to sell raw data. A cybercrime resource site which sells information used for identity theft, *superget.info*, got its data from a data broker named CourtVentures which had a consumers data exchange agreement with another data broker named US Info Search, the original source of the data available through *superget.info*. CourtVentures was acquired by the data broker Experian in 2012, which confirmed an ongoing investigation into the matter [Krebs 2013]. This case clarifies the nature of data-handling practices of data brokers - consumer data is collected, exchanged, aggregated and sold without regard for data subjects. Also, beyond the potential privacy harms, it becomes clear that the data broker industry increases individuals' exposition to identity theft crimes.

6.2.2 Understanding User Behaviour

Despite personal data being used for the ends described in Section 6.2.1, the number of social network and mobile application users continues to grow, as does the revenue of the three key data brokers. Motivated by the seemingly complex and elusive privacy decisions of individuals, the field of privacy economics aims to understand and quantify the costs and benefits that data subjects consider when making privacy choices.

Some scientists in this field assume that people have stable privacy preferences and based on those make well reasoned, coherent privacy trade-off decisions [Acquisti 2009]. These studies view individuals as fully informed and utility maximizing rational economic agents. However, empirical privacy-related research has identified behaviour inconsistent with that model. Data subject claim to be concerned about privacy but act in apparent contradiction with this claim [Acquisti 2004; Acquisti and Grossklags 2005], in a phenomenon coined the *privacy paradox* [Norberg, D. R. Horne, and D. A. Horne 2007]. These systematic inconsistencies suggest that richer theories are required to explain user behaviour. Theories that can accommodate subjects' struggle with inconsistent privacy preferences and frames of judgement, contradictory needs, incomplete information about risks and consequences, and bounded cognitive abilities [Acquisti 2009].

Alessandro Acquisti, from the Carnegie Mellon University, has been a key researcher in de-constructing the user rationality assumption by putting forward evidence that cognitive and behavioural biases highly influence users' privacy decisions. Depending on how these decisions are framed or presented, and what comparisons they evoke, subject choices will vary greatly for essentially the same privacy trade-off. The identified biases are similar to the ones identified in the consumer choice domain [Acquisti 2009].

One study with three experiments focused on the presence of privacy-related queues, conditioning user's privacy concerns for the same decisions [L. K. John, Acquisti, and Loewenstein 2009]. The authors concluded that triggering latent privacy concerns with consent warnings and confidentiality assurances reduced disclosure, while if faced with a frivolous, playful, context subjects will admit to more questionable behaviour. In the third experiment sensitive questions were asked point blank or in a covert way, resulting in significantly more disclosure when the questions were asked covertly.

Another study focused on two consumer choice biases: the endowment effect and the order of choice presentation [Acquisti, L. John, and Loewenstein 2009]. Both effects were observed but results were especially conclusive for the endowment effect: subjects who started from positions of greater privacy protection were five times more likely than other subjects to forego money to preserve that protection.

The most recent study in this area [Brandimarte, Acquisti, and Loewenstein 2012] identified what was coined as the *control paradox*: subject control over the publication of their private data is inversely related to their privacy concerns and directly to their willingness to publish sensitive data. Subjects share more and worry less about privacy when they are in control over the publishing process, suggesting that they mostly value the publication privacy trade-off, while disregarding privacy threats derived from posterior data access and use.

6.2.3 Mitigating the Issues

Assuming the set of economic incentives that motivate personal data gathering and use by companies will not change, it is still possible to mitigate the potential privacy issues that originate from them. This type of privacy issues has a peculiar characteristic that is rarely considered in technical work: the actors that control the ICT infrastructure where the targeted data is stored are themselves are the perpetrators of the privacy attacks. From the user's point of view, data is stored in these systems in order for the user to consume some information or communication service, but according to these service provider's privacy policies that data can be used for the company's economic benefit.

A technical approach that considers this scenario is P3P, analysed in Section 3.4.2. The goal of P3P was to communicate to the user, in a practical way, the contents of web sites' privacy policies so that the users could make informed choices about accessing the said web sites. Economically, the privacy practices of web sites, i.e. how they use data that visitors provide them, can be qualified as a credence good: they cannot be evaluated by the consumer, not even after *consumption* (site visit) - i.e. the user doesn't know how the data gathered about or supplied by him will be handled after accessing a web site, and may come back again even if the data is used for purposes he wouldn't accept. P3P would transform privacy in the web into a search good: users could easily compare it with what they consider acceptable levels or privacy even before the site is visited. However, as already explained in Section 3.4.2, the adoption of P3P hasn't been very successful.

This formulation of privacy, considering all systems as a potential source of attack, is rarely considered in other work. One notable exception is *multilateral security*, which “considers different and possibly conflicting security requirements of different parties and strives to balance” [Rannenberg 2000]. While security typically focuses on protection of system owners against external attackers and misbehaving internal users, protecting external users from operators is not considered a significant issue. The goal is to balance the competing security requirements of different parties that interact with the system. This implies considering that all involved parties are potential attackers. Rannenberg proposes four design strategies for approaching multilateral security:

1. Data Economy: create and transmit as little data as possible (similar to the *data minimization* principle [Pfitzmann and Hansen 2010, p. 6]);
2. Careful Allocation: data allocation in a distributed system should be decentralized, in order to make misuse less attractive and to limit the consequences should it occur, and the party that requires the data security should have the control over said data
3. User ability to control: if users are faced with a trade-off decision between some of their goals, they should be able to understand the situation and control the outcome;
4. Usability of security mechanisms: system should be usable by users at different stages of interest, understanding, and competence.

While these strategies are interesting, an analysis methodology is not provided in multilateral security work. A key reason for this is the nature of the formulations: multilateral security and strategies are phrased in terms of requirements - conflicting ones by different parties, and strategical ones for better overall privacy.

Spiekermann and Cranor recently put forward a set of *privacy-by-architecture* guidelines [Spiekermann and Cranor 2009], more concrete than the multilateral security strategies. They propose two dimensions of architecture that fundamentally impact privacy: network centricity and identifiability. Network centricity is the degree to which a system relies on a infrastructure owned by the network operator or service provider. More network centricity typically means potentially less privacy for clients, but also facilitates the use of inexpensive client devices with minimal storage and processing capabilities. Identifiability can be defined as the degree to which data can be directly attributed to an individual. Spiekermann and Cranor define four privacy stages for identifiability [Spiekermann and Cranor 2009, p. 8]: identified, pseudonymous but linkable with reasonable effort, pseudonymous and unlinkable with reasonable effort, and anonymous.

Network centricity in the privacy-by-architecture approach, similarly to multilateral security, is not measurable. Metrics to analyse the privacy-friendliness of a system from its network distribution and actor incentives point of view have not yet been studied, from all the state-of-the-art that was possible to gather. However some metrics could be given, as it happens with some work in peer-to-peer networks [Buragohain, Divyakant Agrawal, and Suri 2003] and networks of email anonymizers [Acquisti 2003], by economics and game theory. This approach was already theorized by Acquisti [2002] where he suggests that economics can be used to assist in the design process of mechanisms to solve impasses, or assist the user in deciding what data should be shared and protected. However, the evidence showing that modelling user behaviour as a rational agent is a flawed approach, presented in Section 6.2.2, suggests that modelling a representative utility function requires additional empirical research.

Privacy-by-architecture by reducing identifiability, on the other hand, is a well studied and promising approach for mitigating problems caused by economic-driven data aggregation, while maintaining economic benefit for companies. The use of PPDM techniques, discussed in Chapter 5, can enable the reduction of identifiability with reduced functional and economic impact. Specifically, the contribution to PPDM from this thesis, Record Fragentation, discussed in Sections 5.4 and 5.5, has the potential to balance the utility of the gathered high-dimensional data with the risk of privacy harms in case the data is leaked. Datasets resistant to re-identification and with reduced data value for the purposes identity theft and building personal dossiers, would be significantly less appealing to badly intentioned parties.

Despite the described approaches it isn't likely that companies will adopt such mitigation PETs under the current set of assumptions - the cost of re-architecturing existing systems is simply too big. Organizations will only increasingly adopt these technologies if the gain from attracting privacy sensitive costumers, avoiding reputation damage or meeting regulatory requirements is equivalent to the costs [Rubinstein 2012].

6.2.4 Changing the Game

The business models described in Section 6.2.1 define companies' incentives towards the treatment of personal data. The emergence of other, more privacy-friendly, business models would decisively contribute to better privacy practices by companies. While this doesn't happen, service providers will continue to rely in architectures which require users' personal data to be transmitted to their infrastructure, instead of opting for a more client-centric architecture. The network centricity of a service may have important strategic implications for its business model and position in the value chain [Spiekermann and Cranor 2009].

As telecommunication operators, that once aggregated all communications services, in time became *dumb pipes*, maybe web service providers are to become mere logic providers. A project that provides tools to do just that is Remote Storage [2013]: accessing a web page will simply download the application's presentation and logic code, maintaining the properties that made the web a success, while data is stored locally. However, as telecommunication operators are struggling with finding new business models that provide revenue in a converged communications scenario, also providers which give their Internet-based services for free have no clear business alternative to advertising and data licensing.

This key role of personal data in the digital economy is currently well perceived by legislators in the EU. European Commission Vice-President Viviane Reding, EU Justice Commissioner, began contextualizing the EU Data Protection reform as follows [Reding 2012]:

> Personal data is, in today's world, the currency of digital market.

The goals of the EU Data Protection reform aim to improve consumer trust and data portability among e-commerce and Internet businesses, as well as increase transparency of the data handling practices of these companies and reduce bureaucratic burden for them. Transparency of data handling practices may be a key incentive balance change for a number of companies. The public image or even legal problems of some practices may turn out to be an effective deterrent for the most intrusive types of personal data business.

6.3 Role of Law and Regulation

6.3.1 Regulating the Digital Economy

As introduced in Section 2.1.4, personal data is a key asset in the business model of most web companies. So far, US politicians opted to leave consumer privacy issues almost entirely to self-regulation, with limited policing by the FTC [Brown and Marsden 2013, p. 47]. The *laisser-faire* approach of the FTC to the regulation of the digital economy has motivated significant criticism [Solove 2004; Harper 2005], pursuing *a posteriori* a small number of privacy violations, sanctioned with moderate fines [Brown and Marsden 2013, p. 54]. Furthermore, the absence of regulations for the format and language of privacy policies resulted in widespread adoption of policies unintelligible to common consumers [McDonald and Cranor 2008], forcing them to bear too much burden in protecting their privacy [Brown and Marsden 2013, p. 53]. The adoption of more privacy-friendly regulation sin the US has been vigorously fought by ICT company lobbies. Privacy advocates have influenced media and public discourse, and managed to persuade some software companies, namely browser vendors, to work towards improving privacy protections (e.g. P3P, DNT, ...). However, they are typically focused around one technology or use case, and in terms of legislation of regulation they haven't managed victories [Brown and Marsden 2013, p. 62].

The EU Data Protection reform, as mentioned in Section 6.2.4, is anticipated to be a key influence regarding the future rules of the digital economy. Unlike the minimal regulation performed by the FTC in the US, European legislation is placing significant privacy challenges to Internet companies, which are mostly US-based but need to follow EU rules in order to offer their services in the old continent. The interaction between European legislators and these companies has been driving privacy regulation development over the past few years [Brown and Marsden 2013, p. 48]. The feeling of key EU politicians, such as Neelie Kroes and Viviane Reding, is that a balance between business and privacy should be accomplished, in order to avoid a scenario of lost consumer trust in Internet companies and consequently slower adoption of e-commerce and other technologies [Kroes 2010; Reding 2012].

In Europe, governments, legislators and regulators, backed by national Constitutional Courts, the European Court of Human Rights, and the European Parliament, have played key roles in assuring privacy to citizens. Germany in particular has very privacy-friendly legislation, which shaped most of the EU privacy regulations. However, despite being more interventionist and having stronger laws for them than the FTC, EU data protection authorities are usually under-funded and rarely take steps to widely enforce all the privacy requirements [Brown and Marsden 2013, p. 65].

The EU Data Protection reform aims to establish a digital single market in the EU, where data protection regulations are the same, and exempting companies from dealing with several national data protection authorities. On behalf of consumer privacy, it requires companies to provide comprehensible information regarding what data is gathered and how it is processed, and to obtain consent from the users. Also, data portability and the right to be forgotten are to be guaranteed. Finally, in case a data breach occurs, companies are required to report the breach as soon as possible [Reding 2012].

Furthermore, the reform also aims providing clear rules for international data transfers [Reding 2012]. A transfer of data to other countries will be allowed or denied based on how privacy-protecting the laws of the destination country are. Consequently, Europe emerges as a key reference for privacy laws, not only in the academic sense but also because of the practical benefits of being more directly connected to the digital single market [Brown and Marsden 2013, p. 64]. In turn, the US, call for consumer empowerment and dismiss the European way as a bureaucratic and ineffective obstacle to innovation [Brown and Marsden 2013, p. 64]. However, the US-led Asia-Pacific Economic Cooperation (APEC) Privacy Framework, which could represent an international alternative to the European way, failed to be adopted by the countries in the region [Greenleaf 2012].

As of October 2013, the reform documents, a directive and a regulation, were approved in the European Parliament Committee in charge of discussing it. While privacy associations argue the approved documents contain legal loopholes that can exempt companies from many privacy requirements [La Quadrature du Net 2013], the approval deadline of the new data protection laws was delayed to 2015 [General Secretariat of the European Council 2013], following reported digital economy lobbying headed by the United Kingdom [Fontanella-Khan 2013].

6.3.2 Conflicts with Technology

With recent calls for privacy by politicians, *privacy by design* has been hailed as a key enabler of consumer privacy, and as an alternative to overly restrictive legislation and regulation [European Commission 2010; Reding 2012; Federal Trade Commission 2012]. However, as discussed in Section 6.5.1, the exact meaning of the term remains to be specified.

Despite these calls, writing legislation in a technology-neutral way, as it usually happens, makes references to terms like *privacy by design* and *data-minimization* hardly enforceable. As a result, organizations and enterprises have little regulatory incentive to invest in PETs [Bramhall et al. 2007]. However, during the discussions of the EU Data Protection reform in the European Parliament Civil Liberties, Justice and Home Affairs Committee, the distinction between anonymous and pseudonymous data was proposed by some amendments, which deserved a technical recommendation alerting to re-identification problems by the European Data Protection Supervisor [European Data Protection Supervisor 2013]. In case this is a sign that legislators are considering including objective technical requirements in the law, it could represent a significant change of relationship between legislation and technology.

If laws increasingly influence the way ICT are developed, privacy will surely benefit. However, it is important to remember that laws cannot deny the social and technological reality. If certain legal requirements are simply not enforceable then the law should be changed [Langheinrich 2001].

A different type of conflict between technology and law relates to the possible misuses of PETs. The right to privacy is not an absolute right. In certain cases, such as properly mandated judicial inquiry, individual's otherwise private data can be accessed by investigative authorities. The most fundamental PETs, which protect and anonymize communications, do not implement such mechanisms. The same PETs that can be used to more fundamentally protect privacy, such as cryptography and communication anonymity, can also be used to conduct illegal activities. For example, a drug-sale website, accessible through anonymizing communications software Tor, was shut down by US law enforcement recently [Roy 2013]. The investigation that let to the site shut down was successful due to operational security mistakes, as the anonymizing software worked as intended [Tor Project 2013].

6.3.3 Lawfulness and Dangers of Surveillance

The bright side of PETs being ignorant of the law is stressed by the *cypherpunk* movement, introduced in Section 2.1.3. The *Cypherpunk Manifesto* [Hughes 1993] argues that privacy protection cannot be left in the hands of governments, that it must be individually sought after and achieved by technical means such as cryptography. The same PETs that are used to run illegal activity online were also used by Wikileaks, and recently started being adopted by mainstream media, such as Forbes and New Yorker, to protect sources and whistleblowers [Greenberg 2013].

As if self-justifying their own existence, the use of these PETs enabled exposing NSA surveillance practices [Greenwald 2013; Miller 2013b], which have dominated media in the second half of 2013. While some of these practices have been authorized by the US Foreign Intelligence Surveillance Court, there is an ongoing debate regarding the problems of mass surveillance programs [Macaskill and Dance 2013]. Surveillance advocates claim that such practices are necessary to effectively fight terrorism, and have consistently opposed more restrictive privacy legislation. Former intelligence coordinator Sir David Omand wrote that agencies would need blanket access to personal information that resides in databases, and that the "access to such information, and in some cases the ability to apply data mining and pattern recognition software to databases, might well be the key to effective pre-emption in future terrorist cases" [Brown and Marsden 2013, p. 61].

On the other hand, privacy advocates argue that consumer trust, civil liberties and democracy itself are under attack. The collection of phone call metadata alone can reveal significantly about a person's intimate life, and according to the American Civil Liberties Union, such information should not be accessible to the government without good reason [Macaskill and Dance 2013, Section 2]. The absence of a public debate on surveillance laws and the secret interpretations of the existing ones without proper democratic control [Macaskill and Dance 2013, Section 5] strengthens the long existing fears of Orwellian and Kafkaesque scenarios becoming reality (see Section 2.2.5). Finally, in line with the European politicians' fears regarding public image of the ICT industry [Kroes 2010; Reding 2012], US congresswoman Zoe Lofgren fears a consumer backlash on US companies in case they keep being leveraged for mass surveillance programs [Macaskill and Dance 2013, Section 3].

The absence of clear leadership in the EU regarding collaborations on the field of intelligence gathering led the US to criticize the European Commission in 2009, as national data protection authorities regularly make independent public statements [Brown and Marsden 2013, p. 61]. Recently, following revelations of NSA surveillance on European Heads of State and Government [Ball 2013], France and Germany stated interest in seeking bilateral talks with the US before the end of 2013 in order to reach an understanding on mutual relations in the field intelligence field [General Secretariat of the European Council 2013].

However, NSA surveillance does not restrict itself to EU leaders, also including mass surveillance of citizens [Greenwald and Aranda 2013], reportedly aided by European espionage agencies [Borger 2013]. While the ongoing work on EU Data Protection reform can make surveillance based on service provider data less effective, as restrictions are introduced regarding the physical location of data centres, mass surveillance done with the collaboration of domestic intelligence remains unaffected. Europe cannot be a spectator of the US public discussion regarding the limits of intelligence agencies activity, nor regarding its international intelligence agreements. The potential penalty for this is continued decrease of citizen trust in governments and increasing adoption and responsibility for PETs.

6.4 Privacy in the Information Society

6.4.1 Media Understanding of Privacy

In order to better perceive the global understanding of privacy issues by mainstream media, an analysis to the New York Times news archives was conducted. A total of 4784 privacy related news articles were considered, ranging from November 1980 to July 2015. Their year and tags were used to conduct a frequency analysis. The 30 most common all-time tags are depicted in Table 6.1, along with how frequently they show up in privacy-related articles. The most common tag, *computers and the internet*, shows up associated to privacy news for the first time only in 1999, maintaining after that a meaningful average frequency of 40%. Another ICT-related tag, *computer security*, starts being used in 1995 while *telephones and telecommunications* has its first use in 1993. The most relevant ICT-related tag before 1995 is *data processing (computers)*, which shows up consistently (average of 9%) in the 1980's and early 1990's, but is rarely used after 1995. Regarding the nature of privacy issues, the most common tag is *terrorism*, which has an especially high average of 20% frequency from 2001 to 2013, illustrating how much 9/11 influenced the public discussion around privacy.

Table 6.2 shows the top simultaneous tag occurrences, showing correlations between tags. It's clearly identifiable the correlation between the tags *terrorism*, *surveillance of citizens by government* and *wiretapping and other eavesdropping devices and methods*. A distinct group of tags that emerges in the top occurrences of the tags frequently accompanying *computers and the internet*, which include *computer security*, *google inc*

Table 6.1: Top 30 tags in privacy-related news articles (1980-2015)

1.	computers and the internet	27.52%	16.	disclosure of information	5.03%
2.	privacy, right of	22.82%	17.	bush, george w	4.95%
3.	law and legislation	17.43%	18.	search and seizure	4.80%
4.	terrorism	11.97%	19.	editorials	4.72%
5.	united states	11.45%	20.	supreme court	4.70%
6.	surveillance of citizens by government	11.24%	21.	google inc	4.66%
7.	suits and litigation	9.78%	22.	news and news media	4.66%
8.	wiretapping and other eavesdropping devices and methods	7.14%	23.	national security agency	4.61%
9.	computer security	7.00%	24.	clinton, bill	4.41%
10.	decisions and verdicts	6.43%	25.	consumer protection	4.36%
11.	ethics	6.25%	26.	united states politics and government	4.28%
12.	telephones and telecommunications	5.95%	27.	sex crimes	4.13%
13.	new york city	5.43%	28.	tests and testing	3.88%
14.	medicine and health	5.28%	29.	regulation and deregulation of industry	3.78%
15.	security and warning systems	5.20%	30.	electronic mail	3.67%

Table 6.2: Top 10 Simultaneous Tag Occurrences in Privacy-Related News Articles (1980-2015)

1.	law and legislation	united states	8.44%
2.	surveillance of citizens by government	terrorism	6.77%
3.	computers and the internet	computer security	5.72%
4.	disclosure of information	privacy, right of	5.03%
5.	surveillance of citizens by government	wiretapping and other eavesdropping devices and methods	4.66%
6.	terrorism	wiretapping and other eavesdropping devices and methods	4.49%
7.	law and legislation	privacy, right of	4.32%
8.	national security agency	surveillance of citizens by government	4.20%
9.	computers and the internet	law and legislation	4.07%
10.	computers and the internet	google inc	3.86%

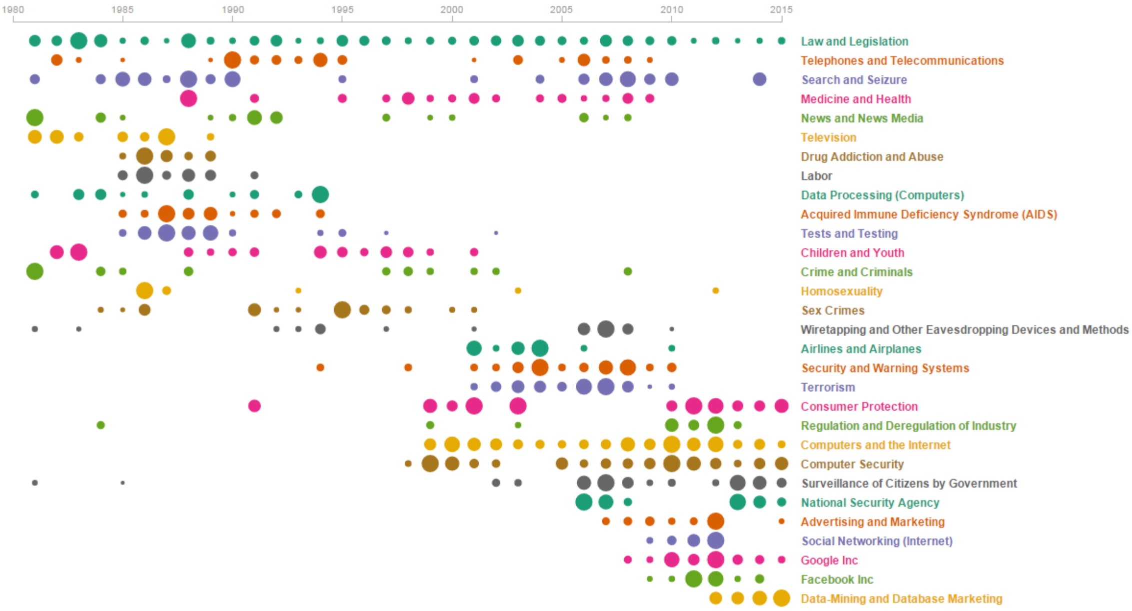

Figure 6.1: Tag relevance over time for New York Times privacy-related articles from 1980 to 2015

and *advertising and marketing*. This suggests that privacy issues are mainly distinguishable in two key classes: government surveillance and company customer profiling. The tag *law and legislation* shows up with all the other top tags, meaning that it is a tag with little distinctive value, as is the tag *united states*.

Figure 6.1 [Gonçalves 2015] shows the evolution of some popular tags over the years (tags related to location and people were disregarded), showing clear changes over time for many topics, while others that exhibit some stabiliy. The tags that show up consistently over time are shown on top. In the 1980s and begining of 1990s, privacy issues appear significantly related to issues regarding sensitive information (e.g. drug abuse, AIDS and sex crimes). In the second half of the 1990s technology-related tags start gaining relevance. The 2000s were deeply marked by terrorism and the American response to it, which involved increased surveillance and aggressive intelligence gathering. The same period also marks the establishment of ICT as the main privacy arena. Since 2010, privacy in the Web clearly has the spotlight. The business model

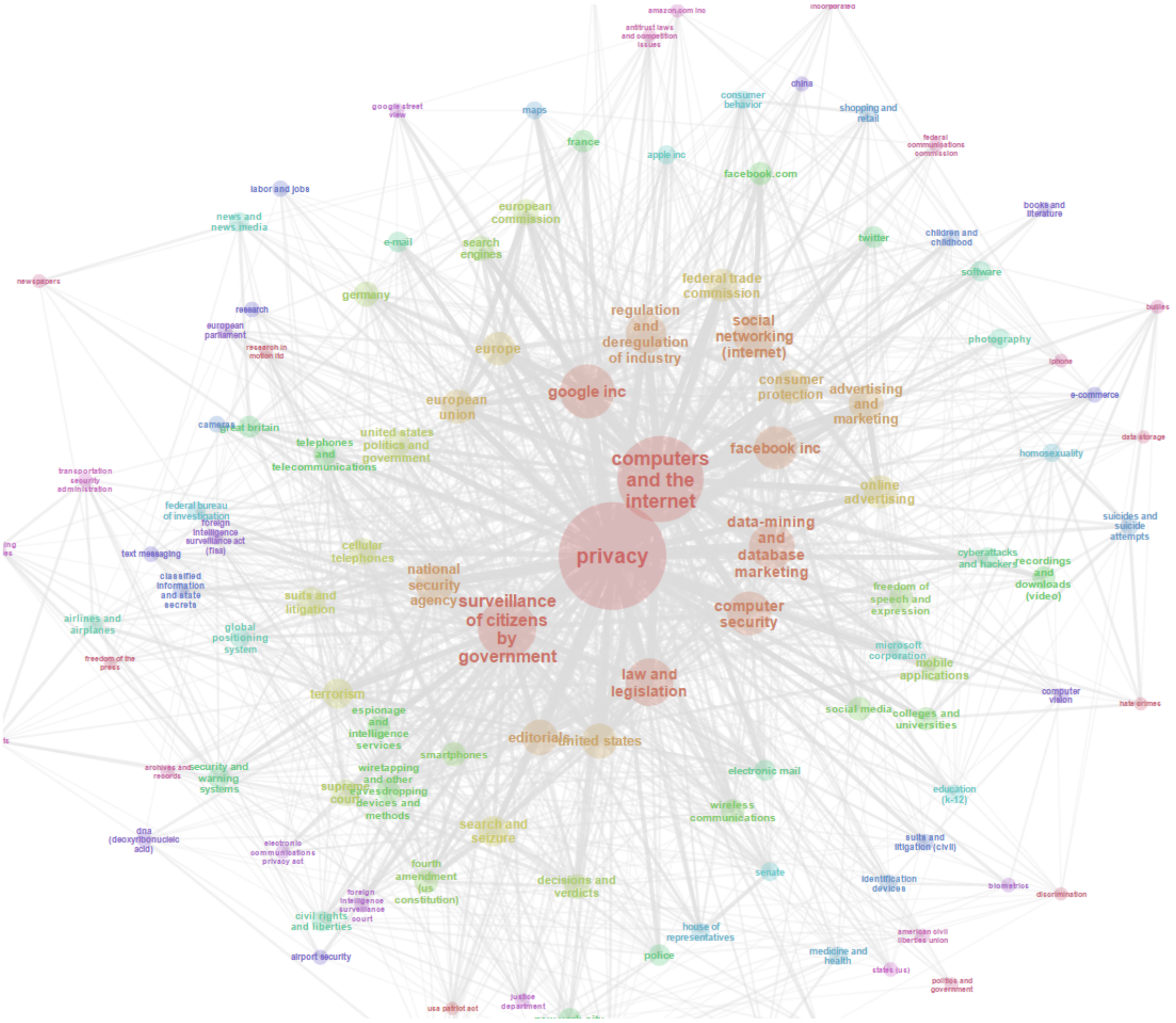

Figure 6.2: Tag graph for New York Times privacy-related articles from 2009 to 2015

of the Web giants Google and Facebook has raised a number of privacy concerns, as introduced in Section 2.1.4 and further discussed in Section 3.4.2.

From the types of actors that create privacy issues identified in Chapter 2, individuals, companies and governments, issues created by individuals are the least visible in the analysed data. On the other hand, the importance of technology as well as the two different types of privacy threats that government and companies create, are clearly represented. Figure 6.2 [Gonçalves 2014] shows a tag graph for the tags in the articles of 5 recent years, that confirms just that. Size of the nodes indicates number of occurrences, while distance and thickness of links indicates number of co-occurrences. It's clearly identifiable the correlation between the tags *national security agency* and *surveillance of citizens by government*, related to state surveillance. A distinct group of tags is visible around *computers and the internet*, ranging from *google inc* to *data mining and database marketing*, the tags most related to the digital economy.

6.4.2 The Role of Social Practice

From the results presented in Section 6.4.1 it's possible to observe wide public discussion regarding privacy problems caused by governmental security and intelligence agencies and by companies that operate in the digital market. However, privacy abuses committed by individuals aren't usually discussed. As introduced in Section 2.2.5, this type of privacy issues is also enabled by technology. Users may use it to actively seek private information of others, such as it is feared to happen with Google Glass [Miller 2013a; Streitfeld 2013], or it may mislead users into releasing information in inappropriate ways. In a survey where 55% of Internet users said they had taken steps to avoid being observed online, their adversaries were predominantly hackers, advertisers and people they personally knew, rather than companies, government or law enforcement [Rainie et al. 2013]. This shows the relevance of individual privacy for users, despite its residual media coverage.

As noted in Section 2.2.4, Warren and Brandeis' privacy legal work from 1890 [1890] was prompted by a technology advance that would enable individuals to take pictures of others without requiring their permission. Today, similar problems are being discussed, prompted by the presentation of Google Glass. The US Congress asked for clarification regarding Google Glass' potential for privacy infringement of individuals, namely regarding its ability to record video and audio inconspicuously, and its potential facial recognition capabilities [Barton et al. 2013]. This type of privacy fears will only be made worse by the progress of technology, extending natural human ability.

However, social practice has a role to play. There are currently numerous establishments, most commonly casinos and night clubs, which don't allow the use of photographic cameras, and the same could happen for wearable devices such as Google Glass [Streitfeld 2013]. Thad Starner, a key figure on Google's Project Glass, was quoted by the New York Times saying that "asocial people will be able to find a way to do asocial things with this technology, but on average people like to maintain the social contract." [Streitfeld 2013]. In a recent article about Glass, Starner [2013] stresses the importance of *microinteractions* as devices merge with everyday objects, and places privacy emphasis in implementing microinteractions that are transparent to bystanders, encouraging socially appropriate use.

Already part of reality is the emergence of new social privacy practices and skills from the use of social networking sites. The user's understanding of their actions online is bound to improve with time, leading to more rewarding online experiences with less privacy-related harms. The Pew Research Center report *Teens, Social Media, and Privacy* [Madden et al. 2013] shows data that allows for such optimism: while online sharing in social networks done by teenagers has increased significantly since 2006, a majority (57%) of them reports positive experiences, while 17% reporting having felt scared or uncomfortable and under 8% reporting actual problems due to over-sharing. These teens also have Facebook friendship networks that largely mirror their offline networks, report high privacy control ability and actively manage their online image by editing and deleting content, all re-enforcing the idea that day-to-day individual exercise of privacy is gradually being transferred to the online world. Teens with large networks share a wider range of content, but are also more active in profile pruning and reputation management activities.

Starner believes that interaction design can shape future social practices with Google Glass. Analogously, existing practices in managing social network image didn't emerge randomly. Technology influenced the emergence of these practices, arguably not always in the best way possible. Lederer et al. [2004], identify a number of cases where existing social practice is inhibited. Despite the reported confidence in managing online image in social networks, a 2011 study shows a significant mismatch between what Facebook users think they have configured as a privacy settings for their photos, and their actual privacy settings. In 907 photos only 332 (37%) were configured with the intended privacy setting, while 443 (49%) were accessible to more Facebook users than the author intended to [Y. Liu and Gummadi 2011]. The same article suggests the use of social proximity information derived from social graphs for assisting user interaction in order to ease privacy setting management. While difficult to get right in new systems, technological support for existing and emerging social practices is of key importance for privacy.

6.4.3 Classification of Privacy Conflicts

In Section 6.4.1 governmental agencies and corporations were identified as key privacy actors from media coverage. These actors have in common that their activities target large groups of individuals. The scale of such data gathering and processing practices is only possible with significant amounts of computing resources and technical knowledge. The individuals potentially harmed by their activities are simply data entries in their system - the relationship between the data subject and holder is deeply asymmetric. In Section 6.4.2 privacy issues in inter-personal relations were described. Here the data subject and data holder have a more symmetric relationship - they maybe even know each other's name. In this case, social norm may come into play and effectively mitigate privacy conflicts, while in the previous, asymmetric, case this is not possible. The motives for the data flow between subject and holder, and possible privacy harms that can come from it, also significantly differ depending on which actors are considered. Table 6.3 groups the privacy conflicts identified throughout the work done in this Thesis in four main contexts, and synthesizes their common actors, motivations and harms. The identified harms take as reference Solove's taxonomy [2006], introduced in Section 2.2.3.

Current State data collection and processing practices create tensions between the State and the civil society, best captured in Section 6.3.3. While reasonable searches and seizures w.r.t. individual suspects of a crime are widely accepted, generalized surveillance may harm the privacy of a society as a whole. This may carry grave consequences to the democratic health of countries, as it enables the State to exert forms political control on a population - an Orwellian scenario. Another danger enabled from State-sponsored surveillance is the birth of a Kafkaesque bureaucracy which prosecutes without humanly justifiable reasons, merely based on data mining outputs. Let us dub this type of privacy conflicts as *surveillance in democracy.* While such conflicts have been common ever since new security practices were adopted to fight terrorism (see Section 6.4.1), the recently uncovered NSA mass-surveillance practices [Macaskill and Dance 2013] changed the landscape of such conflicts. While before mostly activists and whistle-blowers were involved in such issues, now the general population is involved. The data collection and processing practices used by States can be classified as the following privacy harmful activities [Solove 2006] namely: surveillance, aggregation, identification and exclusion. Furthermore, such practices can lead to decisional interference in various ways.

The second type of privacy issues aggregates the ones related to the *digital economy* and the value of personal data. A number of corporations rely on consumer or user data in order to guarantee a revenue stream. These tensions are best captured in Section 6.2.

The data can be used for business analysis, for marketing purposes, or for classification and discrimination in access to credit, price of insurance or being hired. However, users seem unaware of this, as they consistently end up supplying their information to such corporations [McDonald and Cranor 2010]. Also, if the quantity of data amassed by companies is large enough, it becomes economically viable for *black-hat* hackers to attack such companies, seeking monetary gain out of identity thefts. Also, State-sponsored surveillance can resort to similar attack methods and also legal methods to access the user data accumulated by corporations. The list of identifiable privacy harmful activities [Solove 2006] of this type is long:

- surveillance, as some applications collect data without the user's knowledge or consent;
- interrogation, as the access to some service depends on the disclosure or acceptance to disclose some data;
- aggregation, as the amount of data collected by most corporations enables them to profile users with great precision;
- identification, as the amount of data required to profile users usually also identifies them;
- insecurity, as corporations' databases, holding so much personal data for so many users, are high-value targets for *black-hat* hackers and intelligence agencies;
- secondary use, as some corporations make use of data collected with consent for other uses than the ones intended by the user, namely to discriminate regarding access to credit and regarding insurance prices;
- exclusion, as mechanisms for user data access are often not in place;
- disclosure, as some data brokers actually sell user data, namely e-mails and segmentation data, as a product;
- invasion, as some of the data can be used for unsolicited advertising and telemarketing.

The third and fourth types aggregate inter-personal privacy issues. Online communication platforms don't have the offline spatial and temporal barriers - communications can be accessed months or years after the fact, and they can easily reach hundreds of people. The difficulties of managing privacy in a world of *liquid social contexts* is explained in Section 2.2.4. It becomes easy for a user harm his own privacy, by being unable or unwilling to manage appropriately, sharing too much or contextually inappropriate information. Privacy harmful activities [Solove 2006], enabled by social networks and other new communication platforms, include disclosure, increased accessibility and exposure, due to the nature of the communication platform. Interrogation may also be observed, as platform design and sharing norms may induce the user to disclose more than he actually wants. Finally, if some information is disclosed in the wrong context, it may unintentionally distort the image of the data subject towards the new data holders.

The fourth type targets privacy issues relating to the *broken barriers of human perception*, in which an individual actively seeks to get information about another, with the help of technology, for selfish or malicious reasons. In 1890 it was Kodak's snap camera (see Section 2.1), today is Google Glass and RFID - technology advances that can be used to gather information on nearby strangers create new privacy challenges. Information can be gathered through surveillance, in case the information gathering methods do not require the collaboration of the data subject, and interrogation, in

Table 6.3: Contexts of Privacy Conflicts

Context	Data Subjects	Data Holders	Motivations	Harms
Surveillance in Democracy	Civil Society	Government Intelligence Agencies Police	Law Enforcement Intelligence Gathering Counter-Terrorism	Surveillance Aggregation Identification Exclusion Decision Interference
Digital Economy	Consumers and Users	Tech Companies Data Brokers Marketing Companies Insurance Companies Credit Companies Recruitment Companies	Consumer Segmentation Profiling Targeted Advertising Candidate Evaluation Unsolicited Advertising	Interrogation Aggregation Identification Insecurity Secondary Use Exclusion Disclosure Invasion
Liquid Social Contexts	Over-Sharing Individuals	Passive Observers	Communication Attention-seeking Personal/Emotional	Interrogation Disclosure Increased Accessibility Exposure Distortion
Broken Barriers of Human Perception	Passive Individuals	Active Observers	Curiosity Voyeurism Personal/Emotional	Surveillance Interrogation Exposure Appropriation Distortion Blackmail Intrusion

case the the data subject is coerced or tricked into disclose information. Regardless the case, it is likely that intrusion is present in the data gathering moment. Furthermore, the information can be used in a number of malicious ways, namely for exposure, appropriation, distortion and blackmail.

6.5 Technologies and Methods for Privacy-friendly Future Scenarios

6.5.1 Building Privacy-aware Systems

The EU Digital Agenda called for wide application of *privacy by design*, such that "privacy and data protection are embedded throughout the entire life cycle of technologies, from the early design stage to their deployment, use and ultimate disposal" [European Commission 2010, p. 17]. The term *Privacy by design* was initially used in academia by Langheinrich [2001] to designate a set of six principles for guiding privacy-aware ubiquitous system design. The principles are discussions of the well known FIPs in the technological setting of ubiquitous computing:

- notice - data collection cannot go unnoticed, especially in future scenarios where devices used for doing so are practically invisible;
- choice and consent - besides notice, systems that collect data should request consent for doing so from the user, and a choice of not accepting data collection, more than "take it or leave it", should be made available;
- anonymity and pseudonymity - data unlinkable to an individual poses no threat to privacy, but data itself may identify the individual, as discussed in Chapter 5;
- proximity and locality - build safeguards in embedded devices such that they only collect information if their owner is present;

- adequate security - use security safeguards of high resilience for protecting high-value use cases and easy-to-use safeguards for low-value constrained device use cases;
- access and recourse - implement mechanisms in data collection and storage technology that assist legal requirements, such as facilitating privacy policy compliance and detecting violations.

Due to the recent popularization of the term by legislators, the concept was revisited [Davies and Langheinrich 2013]. Faced with the common disregard for privacy functions in ICT systems, the idea is to incorporate privacy principles at design time rather than as an afterthought.

In public policy and law, the term *privacy by design* has been commonly used to convey the general idea of building privacy-friendly systems and processes [European Commission 2010; Cavoukian 2009]. Mentions of the term convey that idea and a variable set principles, but do not specify concrete design and development practices. Motivated by this, Gürses, Troncoso, and Diaz [2011] apply privacy principles in the development process of two projects and attempt to generalize the development activities that were performed within those projects. The result is a set of five engineering activities that lead to more privacy-friendly systems:

- Functional Requirements Analysis - vague or implausible requirement descriptions may force engineers into a design that collects more data, so that posterior changes to system can be accommodated by the design;
- Data Minimization - only the data that is absolutely necessary to fulfil the functionality needs to be analysed and it should be minimized recurring to architectural options and privacy-preserving cryptographic techniques;
- Modelling Attackers, Threats and Risks - once the desired functionality is settled and the data that will be collected is specified, develop models of potential attackers and analyse the likelihood and impact of the identified threats;
- Multilateral Security Requirements Analysis - find a design in which privacy measures and other important security objectives, such as integrity and availability, are accommodated together;
- Implementation and Testing of the Design - implement the solution and test for potential vulnerabilities.

Several iterations of these activities may be required to achieve a privacy-enabled system.

Theses engineering activities are in line with Spiekermann and Cranor's privacy architectural guidelines and rely in the concept of multilateral privacy, as discussed in Section 6.2.3. In fact, additionally to their architectural guidelines, Spiekermann and Cranor also propose a number of recommendations to implement privacy-sensible systems that respect FIPs: *privacy-by-policy* [Spiekermann and Cranor 2009].

With the purpose of helping organizations controlling their systems' privacy features and legal compliance, OASIS proposes the Privacy Management Reference Model and Methodology (PMRM) [Sabo et al. 2012]. PMRM defines a flexible reference model and a number of practices, enabling *privacy by design* because of its analytic structure and operational focus. The considered operational definition of privacy is:

> the assured, proper, and consistent collection, processing, sharing, transmission, minimization, use, retention, and disposition of personal information

> throughout its life cycle, consistent with information protection principles, policy requirements, regulations, and the preferences of the individual.

Another set of privacy practices directed mainly for enterprises are being pursued within the ISO/IEC standards body. ISO/IEC 29100:2011 defines an high-level framework for the protection of personally identifiable information in ICT systems and defines a privacy terminology, a description of actors and roles, and a reference to known privacy principles and safeguarding requirements. ISO/IEC 29101:2013 defines a privacy reference architecture to ease the implementation of privacy safeguarding requirements and to provide guidance for planning, designing and building ICT system architectures that deal with personal information appropriately [Rannenberg 2011].

6.5.2 Holistic View of ICT Privacy

The broad scope of situations that needs to be considered when privacy is being addressed can be challenging to identify. Data can be gathered, processed and disclosed in different technical contexts, and many of these activities are necessary part of the normal execution of ICT services. However, many of these activities also create potential for privacy problems. In Section 2.2.3 Solove's taxonomy for privacy harmful activities is presented, and in Section 6.3.2 these harms were associated with the four main contexts of privacy conflicts identified in this thesis. In Table 6.4 these contexts are matched with the identified privacy-relevant bodies of knowledge from Section 2.3. Below we discuss how the identified bodies of knowledge applies to each type of privacy issues.

Surveillance can be mitigated by the use of techniques that prevent inteligible data to be gathered. The use of cryptography is mandatory to protect communications content, and techniques that enable anonymous communication crucial protection to the existence of communications between two parties. This is mostly applicable to State-sponsored surveillance, but can also be applied when protecting from technologically evolved *paparazzi*. Cryptography, when applied to user data stored by corporations, can also mitigate some privacy harms in case a data leak occurs. With homomorphic encryption, it could further prevent unintended use of data by corporations altogether.

Data-centric and location privacy study the ways privacy can be harmed by the aggregation of data and identification of individuals. Data-centric privacy is applicable whenever large quantities of user data is available: in both data economy and surveillance in democracy cases. Location information has specific gathering and processing techniques which make it worthy of specialized treatment. It is applicable whenever the data holder is capable of somehow gathering location information, whether it is via remote mass-surveillance, disclosure via the use of some service, or individualized local surveillance.

User control of information and behaviour while managing privacy apply mostly to the cases in which users somehow collaborate with the data gathering process. User control of information flows studies the ways users can understand and control information flows in systems, regardless whether they are communication platforms, social networks or gadgets. The study of the choices of users when interacting of such systems is similarly applicable to the *data economy*, *liquid social context* and *broken barriers of human perception cases*. These areas are of key importance because they

Table 6.4: Applicability of Privacy-related Bodies of Knowledge to Different Types of Privacy Issues

	Surveillance in Democracy	Digital Economy	Liquid Social Contexts	Broken Barriers of Human Perception
Cryptography	Content surveillance	Data-leak risks	Not applicable	Content surveillance
Anonymous Communication	Metadata surveillance	Not applicable	Not applicable	Metadata surveillance
Data-centric Privacy	Aggregation and identification	Aggregation and identification	Not applicable	Not applicable
Location Privacy	Identification and aggregation	Identification and aggregation	Not applicable	Identification and aggregation
Privacy in Distributed Systems	Authentication	Disclosure and Accessibility	Accessibility	Authentication and Accessibility
User Control of Information Flows	Not applicable	Disclosure and second use	Understanding of sharing contexts	Understanding of microinteractions
User Behaviour Regarding Privacy	Not applicable	Trade-off data for service	Trade-off reserve for attention	Inter-personal behaviour

may pave the way for new social practices that regulate privacy-related attitudes in these scenarios.

Privacy in distributed systems has to deal with the identities of the network nodes and of the users controlling them. This body of knowledge provides a link between cryptography and control of information. It can be applied in every case as it can mitigate surveillance, through more secure authentication, as well as data disclosure and accessibility, through secure and practical authorization.

6.5.3 Challenges of Future Scenarios

With the realization of AmI, as discussed in Section 2.2.5, many types of data will be collected from everywhere, with great precision. Manual user disclosure will lose it's current relevance and will probably be replaced by coarse privacy controls, enabling or disabling data collection in a specific physical location and time span. Also, the distribution of data collected by one service to third-party services is bound to become widespread, as services rely on each other to provide adaptation functionality.

The possible tactics of IdM, classified according to the amount of data externalized and the identifiability of said data, are anonymity, secrecy, confidentiality and transparency [Smith, Dinev, and H. Xu 2011, p. 9]. However, as future scenarios are considered, characterized by unprecedented data collection and distribution, it's reasonable to assume that the amount of externalized data will be always high, making a confidentiality tactic very difficult to achieve in AmI scenarios. Furthermore, without a scientific breakthrough that enables efficient fully homomorphic encryption, secrecy is also unlikely to be viable. The key goal for protecting privacy will probably be anonymity. Also, considering the four natures of data operations - collection, linking, distribution and aggregation - the most important PETs for the future will be those countering the linking and aggregation of data.

Despite not being able to protect privacy by themselves in future scenarios, technologies that aim controlling the capture and distribution of data will still be required, mostly aiming at data minimization. In order to apply the data minimization principle in a context-awareness scenario a fine-grained access control such as the one proposed in this thesis (Section 4.5) can be used. However its control and parametrization must be assisted, due to its complexity drawn from variety of data collected and services available. Such assistance could be enabled by requiring machine-readable privacy policies to be published by service providers, similarly to P3P, together with an intelligent user interaction agent that appropriately communicates the consequences of privacy choices to users and a coarse manual control.

As it becomes more complex and less effective to micro-control the flow of data, due to the overwhelming quantity of data in circulation, the logical step to take seems to be *hiding in plain sight*. Individuals roam large cities anonymously, as long as they obey to the social norm. If an individual is behaving inappropriately in a public space, attention will be drawn upon him. Similarly, in the digital world, if an anonymous user's data fits existing patterns or clusters, the user is hidden in the crowd. Increased data collection and distribution enables the detection of these patterns and clusters. This information could be used by an IdM mechanism, controlling the linkability between IOI, to estimate uniqueness and tune the linking control. Under this conjecture, the PETs that will have a key impact in the future of privacy will be the ones that work behind the scenes, disrupting data linking and aggregation while requiring little user interaction. However this disruption must not be so aggressive that it prevents the vision of AmI and the benefits of data mining, nor so naive that it allows organizations to discover too much about individuals.

Synergies between the IdM and PPDM fields seem under-explored and present themselves promising ground for future research towards this vision. A holistic approach that tackles linkability and aggregation together, addressing simultaneously distributed systems and data analysis, could be able to deliver an interesting trade-off between functionality and privacy protection. This approach would also enable resistance against data-level re-identification attacks on lower-level identifiers, as explained in Section 3.3.6. A key contribution of this thesis, the concept of Record Fragmentation described in Sections 5.4 and 5.5, is a first step in the direction of addressing privacy simultaneously at both levels. However, the widespread deployment of such a vision would certainly involve addressing identity as a layer, as explored in Section 3.3.5, instead of as an application-level requirement - the current paradigm.

6.6 Conclusions

The concept of privacy itself undergoing transformation. It has changed significantly over the last 40 years, especially in the last decade, and will continue to change as the social and legal debate are faced with new possibilities enabled by technology. The role of personal data in the digital economy is currently being discussed in the political and legal arenas, where the benefits of profiling and data mining have to be weighed against the risks of intrusion [Reding 2012]. At the same time, discussion regarding intelligence gathering practices was triggered by the publication of documents that prove the existence of mass surveillance programs at the NSA [Macaskill and Dance 2013].

A type of issues that deserved less media attention, are the ones that new consumer-grade data gathering technology, such as Google Glass, can create [Miller 2013a; Streitfeld 2013]. This is an area where social practice and human-computer interaction are expected to have most impact. As technology enables individuals to gather more data from their environment and to access remote databases anywhere, the *social design* of new tools becomes increasingly important as they should induce the user in socially-responsible behaviour. If this work is done correctly most people will stick to the social contract [Starner 2013]. Regarding social networking sites, new social practices are emerging as users are becoming increasingly able to manage online personal data and aware of how to work with privacy settings of existing social networks [Madden et al. 2013].

Proficiency in using these new tools leads users to share more data as they get more confident [Brandimarte, Acquisti, and Loewenstein 2012]. The web service providers responsible for these systems take significant care with this as they have economic incentives to motivate users to share more data using their platforms. However, if privacy issues motivated from social awkwardness are avoided, issues based on these companies' business models emerge. Behavioural advertising profiles users and delivers targeted adds, representing a market of many Millions of US dollars [Google Inc. 2013a; Facebook Inc. 2013; Twitter Inc. 2013], while *data brokers* conduct even more questionable data business [Krebs 2013]. While some architectural work exists that doesn't model security and privacy in terms of *good guys vs. bad guys* [Rannenberg 2000; Spiekermann and Cranor 2009], they lack the analytical tools that in some cases can be provided by economics and game theory [Buragohain, Divyakant Agrawal, and Suri 2003; Acquisti 2003], through understanding the incentives of the diverse actors involved in the system. Despite this, without a real change in the economical incentives, it's not likely enterprises will invest in significant privacy improvements. Such a change of incentives could be brought by new regulation or by disruptively different business models.

From the engineering point of view, methodologies and reference models have recently been proposed to aid building privacy-friendly ICT systems [Sabo et al. 2012; Rannenberg 2011]. From the scientific point of view, privacy problems are typically addressed at specific technological contexts, or use cases. Promising work exists in a number of fields, especially for technological contexts that have limited user interaction. This most solid work, however, could benefit from more holistic framing. The most promising ground for progress identified this way is pursuing a joint communications and data approach to privacy, bringing together the fields of IdM and PPDM, following the direction of the work presented in Sections 5.4 and 5.5. Also, in order to pursue data minimization in future scenarios, the work presented in Section 4.5 can be of key importance, together with developments regarding privacy policies for context-awareness scenarios, learning from P3P and from the human-computer interaction field.

Legislation and regulation have the potential to be effective deterrents regarding the economic-motivated privacy problems [Reding 2012], however it's necessary to design them carefully and with technical knowledge. Laws or regulations that try to work against society or that impose unreasonable technical requirements, are bound to cause more problems than solutions [Langheinrich 2001]. Legislation can also be used to implement democratic control to surveillance practices of intelligence agencies, making an appropriate trade-off between security from terrorism and individual privacy [Macaskill and Dance 2013]. However, if individual privacy is essential, as it happens often for political dissidents and activists, technology can offer stronger safeguards than law [Hughes 1993]. However, such PETs can be used both for questioning the *status quo* [Greenberg 2013] and for protection of criminal activities [Roy 2013].

Chapter Seven

Conclusion

Concluding remarks include a summary of results, further research directions and considerations on how to build a more privacy-friendly future.

7.1 Results and Achievements

7.1.1 Overall Achievements

Throughout this thesis privacy was addressed as the true objective, and not as a by-product of security as it is often treated. Its essence was discussed in a multidisciplinary context and a broad range of bodies of knowledge were considered. After introducing the concept and framing the work, privacy was analysed and discussed from the perspective of communications and distributed systems, among which a prototype of an identity layer was implemented as part of the Societies European Project (Section 3.3.5). Following communications work, context-awareness was discussed as a key enabler of the AmI vision of future ICT. Previous work in context-awareness was discussed, and contributions regarding applications (Sections 4.2.3 and 4.3.2), event-oriented context management (Section 4.3.3) and low-latency access control (Section 4.5) were presented. The last perspective used to analyse privacy in ICT was data-centric one, where the PPDM and SDC fields are most relevant. Under this perspective a contribution to the PPDM field, inspired in IdM work, was presented (Sections 5.4 and 5.5).

Finally, a holistic analysis, both socio-economical and technological, was done targeting both the present and near future. The analysis identifies key socio-economic privacy dilemmas, namely public discussion on government surveillance, the economic and regulatory incentives to the handling of personal data by enterprises, and the relations between technological development and social practice that shape individual privacy-related behaviour. The technology landscape is analysed based on data operations and technical context, and the impact of future data collection and distribution practices is taken into account to frame future research.

Such an holistic analysis enables not only the identification of impactful topics for future work, but also establishes relations between work done in different disciplines. Crafting relations between concepts of different fields such as science and technology, law, sociology and economy allows for the emergence of more complete and balanced solutions for privacy issues. Perhaps, most relevantly, legal understanding of technical constraints and vice-versa is of key importance for the shaping of future privacy.

7.1.2 Towards an Identity Layer

Currently the web implements server authentication as part of HTTPS, using an hierarchical PKI, and client authentication as part of the application logic, over HTTPS. This protocol is used mostly as network eavesdropping protection by web service providers, although it is also able to handle client authentication, both using certificates and passwords. However virtually no web service providers use this functionality because of its accessibility and usability problems. User certificates are not easy to manage, and make access from multiple devices non-trivial. Otherwise using HTTPS Basic password authentication involves interacting with browser pop-ups which not convey the ideal user experience. For these reasons, the awkward separation between authentication and encryption became widespread.

The nuisances that the *web of silos* imposes users, namely having to memorize or save one password per web service provider, started to be addressed with the emergence of user-centric IdM, as described in Section 3.3.3. However the currently proposed solutions focus on creating authentication and authorization delegation mechanisms, that similarly operate in the application layer, above HTTPS. However, implementing authentication and authorization as top-level functionality instead of part of an *identity layer* prevents addressing identity and privacy issues that emerge both from the network [Hansen et al. 2004; Matos, Girão, et al. 2007; Matos, Sargento, and Aguiar 2007] and data [Clauβ, Kesdogan, and Kölsch 2005] perspectives.

The contribution to this area was the conceptualization and implementation of an identity-enabled communication layer for the Societies European Project [SOCIETIES 2011; Doolin 2013], as described in Section 3.3.5. XMPP was used as a session-layer protocol where authentication and Identinet [Girão and Sarma 2009] functions are provided, supporting application-layer control and data on top of it. The client-server architecture of XMPP not only enables the Identinet by using the servers and DNS as a resolution mechanism, but also enables servers to act as an anonymizing TTP for most communications. Furthermore, the benefits of this *Identinet* and of a distributed service-oriented ecosystem, which promotes less data aggregation, were published by Gonçalves and Gomes [2014]. Finally, this work enabled application-level payloads to be analysed in the user's device, so that misbehaved applications, sharing more information that they should, are detected [Vardjan and Porekar 2013].

7.1.3 Enabling Privacy-friendly Context-awareness

Context information can be used for enabling many and adapting virtually every ICT service. The development of these future use cases is a challenge that needs to be addressed in different dimensions, from idealizing functionality and business model to devising the enabler architectural choices. As part of the work presented in this thesis, two different scenarios which rely in context information to enable their functionality were proposed in Section 4.2.3: a triggering scenario and a content rating scenario. The Context-aware Triggering System [Simões et al. 2009] can be an enabler for reactive services such as geo-targeted advertising, triggering a configurable reaction to an event, or a standalone application directed to convergent telecommunications operators. The Context-aware Content Rating [Gonçalves, Delahaye, and Lamorte 2010] scenario enables ranking of multimedia content, both professional and user-generated, using change-prone context information, instead of static rating information as used by traditional recommendation systems. The architectural components required for their implementation following service-oriented principles are described in Section 4.3.2.

However, in order to enable adaptation scenarios for improving human interaction with systems, the latency limits of end-to-end context delivery are bound by human perception and reaction times. In order to meet such tight requirements, an event-driven context management platform was developed [Gomes et al. 2010] which uses XMPP as the main communication protocol because it transparently provides federation and PubSub functionality. The platform is described in Section 4.3.3. Similarly to previous approaches it enables the de-verticalization of context-aware applications, but it does so in a way that it privileges speed of context update propagation, taking reactive capabilities to the near real-time level.

As follow-up work, an access control mechanism was devised for the event-driven platform [Gonçalves, Gomes, and Aguiar 2012], extending the existing architecture, as described in Section 4.5. The resulting system complies with the real-time constraints of event-driven context management, adding approximately 20ms to a process that must take under 190ms. This access control scheme supports complex decisions based on both context value and metadata, such as time and type, in an extensible setting. The access control policies are enforced at subscription time, and the context distribution resources are re-configured as the policies change, leaving only quick validations to be performed on context update.

7.1.4 A Different Approach to Privacy-preserving Data Mining

Personal information aggregated in datasets can represent serious privacy threats, namely re-identification and sensitive attribute disclosure, if not appropriately protected. For this reason there are a number of techniques studied in the PPDM and SDC fields that aim protecting against such threats while preserving the dataset utility for the purposes it was originally aggregated. However, in the high-dimensional case, the number of attributes in the dataset is so high that all records are very distinguishable, making them especially vulnerable to re-identification. The application of existing methods to protect against re-identification in the high-dimensional case would render the dataset practically useless.

An achievement of the work done in the scope of this thesis is the exploration of a method for high-dimensional datasets that preserves utility for the key data mining workloads applied to this kind of datasets.This method, inspired in IdM work and described in Section 5.4, protects against re-identification vulnerability and impact by using pseudonym-style data partitioning, fragmenting each record - set of attribute values referring to the same user - in several disjoint records. The method was applied to two well known movie recommendation datasets, Netflix and Movielens, and the impact in utility and re-identification success and impact was evaluated. The results, detailed in Section 5.5, show that a limit to re-identification success rate is imposed, and that the attack pay-off is greatly reduced, while introducing acceptable error in data mining predictions.

7.2 Future Work

7.2.1 Communications and Data Perspectives Towards a Privacy-enhancing Identity Layer

As described in Section 6.5.3, the overwhelming increase of data flows foreseen for future scenarios makes it increasingly interesting to focus in anonymity, to take a privacy approach of hiding individuals in the crowd. A holistic approach that draws on existing aggregated information to estimate how distinguishable is a digital partial identity, and accordingly adjust the linkabilility decisions for that digital partial identity. The trade-off between functionality and privacy could be better estimated due to the metrics provided by the aggregated information. Such an approach could resist data-level re-identification attacks by adapting the concept of Record Fragmentation, described in Sections 5.4 and 7.1.4, to live use. The resistance to data-level re-identification, that can be provided by the field of PPDM to the field of IdM, is essential for future scenarios.

This would involve the development of new PPDM work in two foreseeable directions. First in a theoretical direction, working in a solid mathematical model, similar to the work by Chawla et al. [2005] and Dwork [2011], that can model re-identification in multiple partial identity cases. Second, a more practical direction that involves more empirical experimentation of existing PPDM work such as condensation [C. C.

Aggarwal and Yu 2004]. However, there are data characteristics that are not captured by current work in PPDM. The quasi-identifier assumption hides the problem of understanding how identifying is some type and values of data. However, in a scenario where data is permanently collected from multiple sources, it may be possible to draw statistical characteristics from the data of a specific type that can help quantify how distinguishable it is, both in general and regarding specific ranges of values. Not only individual values are relevant, but also the variation of values in time, as it happens with location privacy analysis described in Section 2.3.5. Despite being dense work, this type of data characterization, significantly drawing from information theory, would help to further build the necessary knowledge for extending current PPDM generic approaches.

On the IdM side, only an identity layer built in between transport and application layers, like the one idealized in Section 7.1.2, is able to conveniently control linkability. Besides enabling useful network abstractions, it enables that data flows controlled by applications in the context of a partial identity to be audited by the client-side identity-layer component, such as done by Vardjan and Porekar [2013]. Knowing what data flows in what identity context to what remote entities is key to estimate how linkable are the different partial identities of an individual, based on the discussed PPDM work. Furthermore, threats to linkability coming from the network would only have to be addressed with respect to this layer, not requiring a complete vertical approach, including application layer, such as the one proposed by Matos, Girão, et al. [2007] and Matos, Sargento, and Aguiar [2007].

7.2.2 Data Minimization in Context-awareness Scenarios

While the results presented in Section 7.1.3 are readily applicable, the path to data minimization in context-aware systems, as described in Section 6.5.3, is still long. The control of the access control system described in Section 4.5 in a scenario with numerous CxP and CxC available, requires assistance from other techniques. One possible way is to require the CxC to publish machine-readable privacy policies, not only describing their internal practices as it happens with P3P, but also with measures of the required QoC for the adaptation or activation of the associated service. Making privacy a search good (see Section 6.2.3) could foster competition among CxC towards requiring less precise context information while delivering equivalent functionality.

Also, existing QoC work and context obfuscation techniques could be greatly enriched with contributions from data-centric bodies of knowledge. Context obfuscation, for example, is typically done through a form of generalization used PPDM, and it would certainly benefit from insights gathered in that field. Finally, some work from the field of human-computer interaction, such as an intelligent user interface that non-intrusively obtains the user privacy preferences based on his usual choices, as suggested for example by Papadopoulou et al. [2008]. The interaction design for context-awareness control should consider the guidelines laid out by Lederer et al. [2004], namely including a coarse manual control.

7.2.3 Economics and Game Theory for Multilateral Architectures

The concept of network centricity, discussed in Section 6.2.3, conveys the degree to which a system relies on a infrastructure owned by the network operator or service provider. More network centricity generally means less data control for users. The concept depicts a key architectural trade-off between functionality and data which must be on the provider side and which can remain on the consumer device. This concept can be seen as a specialization of the multilateral principle of “Careful Allocation” [Rannenberg 2000, p. 10] for the currently widespread client-server model: since the user is the party requiring security for his personal data, he should have the control over said data. However, in the development of systems, this principle has to be balanced with a number of other requirements which are usually more important from the provider’s point of view.

The independent, multilateral, analysis of architectures is a barely explored field. The study of the incentives of actors under a specific architecture has been rarely done, and the few existing cases have focused in peer-to-peer scenarios. Buragohain, Divyakant Agrawal, and Suri [2003] used the game theory notion of *Nash Equilibrium* to analyse the strategic choices done by the peers of a peer-to-peer file sharing system, and use a differential service incentive scheme in order to attempt raising the overall availability of the system. In a privacy-related application, Acquisti [2003] explores the incentives of actors to participate as senders and nodes in mix-net communication anonymizers. These instruments of economic analysis could be useful for evaluating architectures based on multilateral principles, especially hybrid ones which are not purely peer-to-peer nor client-server, or those that would normally require the involvement of a TTP.

7.3 Recommendations for a Privacy-aware World

7.3.1 Re-defining the Digital Economy

The digital economy, with personal data as its currency [Reding 2012], is currently being discussed in the political and legal arenas. The EU Data Protection reform bids to understand both consumers and businesses perspectives. Consumers have to weigh the benefits of data mining against the risks of intrusion , while innovative ICT businesses have to generate revenue while respecting regulations and consumer trust [Reding 2012]. The digital economy, described in Section 2.1.4, uses personal data in numerous marketing-related business models, from targeted advertising to direct marketing based on consumer segmentation.

The directive and regulation being discussed in the EU as part of the Data Protection reform is expected to place significantly tighter restrictions in business operations than its US counterpart, a *laisser-faire* approach enforcing the FIPs from the FTC. Despite this, and despite significant resistance and lobbying against the tightening of Data Protection in the EU [Fontanella-Khan 2013], privacy advocates continue asking for stronger privacy protection from this legislative effort [La Quadrature du Net 2013], as discussed in Section 6.3.1. EU politicians will have to balance the interest of European consumers and their single market with the economical prosperity of an ICT sector which is currently dominated by companies based in the US. As a key goal of the EU is to strengthen the European Internet-based businesses the Data Protection reform may create an opportunity for European competitors to conquer some user-base to their American counterparts.

Regardless of the balance found by politicians, data protection laws will only be effective if they are tech-savvy. As discussed in Section 6.3.2, technology cannot be ignored by legislation under the risk of being ignored back. If efforts such as the work by Gürses, Troncoso, and Diaz [2011], and this very thesis, fail to mediate understanding between the two domains, whatever law that is passed will have little impact for two key reasons. First, because in the absence concrete technical requirements, organizations and enterprises have little regulatory incentive to invest in PETs [Bramhall et al. 2007], otherwise turning their investment to their legal departments. Second, because the legislation requirements may be out of phase with technical reality, imposing restrictions which are too costly or even impossible to enforce [Langheinrich 2001].

Data-centric privacy-preserving techniques, such as the ones discussed in Chapter 5, can significantly help reducing the privacy risks associated with data aggregation. As data becomes less usable for other purposes than the intended, it will also be less appealing to be attacked by hackers, disgruntled employees or the company itself, in a future situation of financial problems. As the uses of personal data should be known at data collection time, the anonymization method presented in this thesis (see Sections 5.4 and 5.5) is a possible candidate to such risk reduction procedures.

However, as discussed in Section 6.2.4, only the emergence of alternative business models that do not require personal data have the potential to drastically change the landscape for privacy in ICT. As telecommunication operators, that once aggregated all communications services, in time became *dumb pipes*, maybe web service providers are to eventually become mere logic providers that get their revenue by crowdfunding.

7.3.2 Surveillance and Democracy

As shown in the results presented in Section 6.4.1, governmental security and intelligence agency surveillance practices started being commonly discussed in the US media as a privacy issue since the 2000s, prompted by the security programmes designed by the Bush administration to fight terrorism in the aftermath of 9/11. Recently the NSA mass surveillance practices became publicly known [Greenwald 2013; Miller 2013b; Macaskill and Dance 2013], dominating media attention thereon, as discussed in Section 6.3.3.

Mass surveillance of citizens by government aims to detect possible terrorist activity patterns through data mining and enacting pre-emptive measures to thwart the efforts of these supposed terrorists [Brown and Marsden 2013, p. 61]. This current vision of intelligence agencies is dangerously close to Kafka's conceptions from *Der Prozess*, presented in Section 2.2.5, where individuals are prosecuted by an uncountable bureaucratic organism which does not clearly state the crimes the individuals have to answer for.

Intelligence agencies require having secret activities but they must be subject to strict democratic controls. The current surveillance debate in the US, as described in Section 6.3.3, should be attentively followed by Europe as this is also Europe's problem: mass surveillance of European citizens by the NSA [Greenwald and Aranda 2013] was reportedly done with the help of European intelligence agencies [Borger 2013]. An internal EU debate has to occur in parallel with the one of the US, that decides on the necessary democratic safeguards to the surveillance practices of European agencies.

The strongest safeguard against even greater dangers of surveillance, such as Orwellian control or political censorship, are PETs that do not require trusting governments or businesses. These PETs besides also being used to conduct illegal activities, as discussed in Section 6.3.2, are tools that safeguard essential freedoms. The anonymizing communications software Tor, which has been recently used to hide the conduction of illegal activities [Roy 2013], was before used to bypass the Chinese government Internet control [D. Anderson 2012]. The resilience of these technologies may very well be the characteristic that makes them be targeted by surveillance advocates but, considering the proportionality principle, it is not acceptable in democracy to attempt to criminalize or otherwise disrupt the use of these tools, that assure such essential freedoms, with the purpose of hindering criminal activity that occurs through them. It is of up-most importance to preserve their legality and support their development.

Bibliography

Abdul-Rahman, Alfarez (1997). “The PGP Trust Model”. In: *EDI-Forum: the Journal of Electronic Commerce* 10.3, pp. 27–31.

Abowd, Gregory D. et al. (1999). “Towards a better understanding of context and context-awareness”. In: *Lecture notes in computer science*, pp. 304–307.

Acquisti, Alessandro (2002). “Protecting privacy with economics: Economic incentives for preventive technologies in ubiquitous computing environments”. In: *Proceedings of Workshop on Socially-informed Design of Privacy-enhancing Solutions, 4th International Conference on Ubiquitous Computing (UBICOMP 02).*

— (2003). “On the economics of anonymity”. In: *Financial Cryptography.* Springer Berlin Heidelberg, pp. 84–102.

— (2004). “Privacy in electronic commerce and the economics of immediate gratification”. In: *Proceedings of the 5th ACM conference on Electronic commerce*, pp. 21–29.

— (2009). “Nudging privacy: The behavioral economics of personal information”. In: *Security & Privacy, IEEE* 7.6, pp. 82–85.

Acquisti, Alessandro and Jens Grossklags (2005). “Privacy and rationality in individual decision making”. In: *Security & Privacy, IEEE* 3.1, pp. 26–33.

Acquisti, Alessandro, L John, and George Loewenstein (2009). “What is privacy worth”. In: *Twenty First Workshop on Information Systems and Economics (WISE).*

Adam, Nabil R. and John C. Worthmann (1989). “Security-control methods for statistical databases: a comparative study”. In: *ACM Computing Surveys (CSUR).*

Adomavicius, Gediminas and Alexander Tuzhilin (2005). “Toward the next generation of recommender systems: A survey of the state-of-the-art and possible extensions”. In: *IEEE transactions on Knowledge and Data Engineering* 17.6, pp. 734–749.

Aggarwal, Charu C. (2005). “On k-anonymity and the curse of dimensionality”. In: *Proceedings of the 31st international conference on Very large data bases*, pp. 901–909.

Aggarwal, Charu C., Alexander Hinneburg, and David A. Keim (2001). “On the surprising behavior of distance metrics in high dimensional space”. In: *Proceedings of the ICDT Conference*, pp. 420–434.

Aggarwal, Charu C. and Philip Yu (2004). “A condensation approach to privacy preserving data mining”. In: *Advances in Database Technology-EDBT 2004*, pp. 183–199.

Aggarwal, Gaurav et al. (2010). “An Analysis of Private Browsing Modes in Modern Browsers.” In: *USENIX Security Symposium.*

Agrawal, Dakshi and Charu C. Aggarwal (2001). “On the design and quantification of privacy preserving data mining algorithms”. In: *Proceedings of the twentieth ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems*, pp. 247–255.

Aguiar, Rui L. et al. (2006). "Identity management in federated telecommunications systems". In: *Proceedings of the Workshop on Standards for Privacy in User-Centric Identity Management 2006*.

Anderson, Daniel (2012). "Splinternet Behind the Great Firewall of China". In: *ACM Queue* 10.11.

Anderson, Ross (1996). "The Eternity Service". In: *Pragocrypt'96*, pp. 242–252.

Ardagna, Claudio A. et al. (2007). "Location privacy protection through obfuscation-based techniques". In: *Data and Applications Security XXI*. Springer Berlin Heidelberg, pp. 47–60.

Arkko, Jari and Pekka Nikander (2004). "Weak authentication: How to authenticate unknown principals without trusted parties". In: *Lecture Notes in Computer Science* 2845, pp. 5–19.

Article 29 Data Protection Working Party (2013). "Opinion 04/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force". URL: `http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp205%5C_en.pdf`.

Atkins, Derek, William Stallings, and Philip Zimmermann (1996). *RFC 1991: PGP Message Exchange Formats*. URL: `http://tools.ietf.org/html/rfc1991`.

Atzori, Luigi, Antonio Iera, and Giacomo Morabito (2010). "The Internet of Things: A survey". In: *Computer Networks* 54.15, pp. 2787–2805.

Ball, James (2013). *NSA monitored calls of 35 world leaders after US official handed over contacts*. URL: `http://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls`.

Barbaro, Michael and Tom Zeller Jr (2006). *A Face Is Exposed for AOL Searcher No. 4417749*. URL: `http://select.nytimes.com/gst/abstract.html?res=F10612FC345B0C7A8CDDA10894DE404482`.

Barisch, Marc et al. (2010). "Security and privacy enablers for future identity management systems". In: *Future Network and Mobile Summit 2010*.

Barkhuus, Louise and Anind K. Dey (2003). "Location-based services for mobile telephony: a study of users' privacy concerns". In: *Proceedings of the INTERACT 2003, 9TH IFIP TC13 International Conference on Human-Computer Interaction*. Vol. 2003, pp. 709–712.

Barton, Joe et al. (2013). *Google Glass Letter to Larry Page*. URL: `http://joebarton.house.gov/images/GoogleGlassLtr%5C_051613.pdf`.

Bauer, Kevin, Dirk Grunwald, and Douglas Sicker (2009). "Predicting Tor Path Compromise by Exit Port". In: *Performance Computing and Communications Conference (IPCCC), 2009 IEEE 28th International. IEEE*, pp. 384–387.

Bauer, Kevin, Damon McCoy, et al. (2007). "Low-resource routing attacks against tor". In: *Proceedings of the 2007 ACM workshop on Privacy in electronic society*. ACM, pp. 11–20.

Bellare, Mihir, Viet Tung Hoang, and Phillip Rogaway (2012). "Foundations of garbled circuits". In: *Proceedings of the 2012 ACM conference on Computer and communications security*. ACM, pp. 784–796.

Benisch, Michael et al. (2010). "Capturing location-privacy preferences: Quantifying accuracy and user-burden tradeoffs". In: *Personal and Ubiquitous Computing* 15.7, pp. 679–694.

Beresford, Alastair R. and Frank Stajano (2003). "Location privacy in pervasive computing". In: *IEEE Pervasive Computing* 2.1, pp. 46–55. ISSN: 1536-1268. DOI: `10.1109/MPRV.2003.1186725`.

— (2004). “Mix zones: User privacy in location-aware services”. In: *Pervasive Computing and Communications Workshops, 2004. Proceedings of the Second IEEE Annual Conference on*, pp. 127–131.

Berkovsky, Shlomo et al. (2007). “Enhancing privacy and preserving accuracy of a distributed collaborative filtering”. In: *Proceedings of the 2007 ACM conference on Recommender systems.* URL: `http://dl.acm.org/citation.cfm?id=1297234`.

Beyer, Kevin et al. (1999). “When is “nearest neighbor” meaningful?” In: *Proceedings of the ICDT Conference*, pp. 217–235.

Bilton, Nick (2010). *Price of Facebook Privacy? Start Clicking.* URL: `http://www.nytimes.com/2010/05/13/technology/personaltech/13basics.html`.

— (2012). *Facebook Changes Privacy Settings, Again.* URL: `http://bits.blogs.nytimes.com/2012/12/12/facebook-changes-privacy-settings-again/`.

Bilton, Nick and Brian Stelter (2011). *Sony Says PlayStation Hacker Got Personal Data.* URL: `http://www.nytimes.com/2011/04/27/technology/27playstation.html`.

Borger, Julian (2013). *GCHQ and European spy agencies worked together on mass surveillance.* URL: `http://www.theguardian.com/uk-news/2013/nov/01/gchq-europe-spy-agencies-mass-surveillance-snowden`.

Borisov, N, Ian Goldberg, and Eric Brewer (2004). “Off-the-record communication, or, why not to use PGP”. In: *. . . of the 2004 ACM workshop on Privacy . . .* URL: `http://dl.acm.org/citation.cfm?id=1029200`.

Boyd, Danah M. (2002). “Faceted id/entity: Managing representation in a digital world”. PhD thesis. Massachusetts Institute of Technology. URL: `http://www.danah.org/papers/Thesis.FacetedIdentity.pdf`.

Brakerski, Zvika and Vinod Vaikuntanathan (2011). “Fully homomorphic encryption from ring-LWE and security for key dependent messages”. In: *Advances in Cryptology–CRYPTO 2011.* Springer, pp. 505–524.

Bramhall, Pete et al. (2007). “User-centric identity management: new trends in standardization and regulation”. In: *Security & Privacy, IEEE* 5.4, pp. 84–87.

Brandimarte, Laura, Alessandro Acquisti, and George Loewenstein (2012). “Misplaced confidences: Privacy and the control paradox”. In: *Social Psychological and Personality Science* 4.3, pp. 340–347.

Brickell, Justin and Vitaly Shmatikov (2008). “The cost of privacy: destruction of data-mining utility in anonymized data publishing”. In: *14th ACM SIGKDD International Conference on Knowledge discovery and data mining.*

Brown, Ian and Christopher T. Marsden (2013). *Regulating Code: Good Governance and Better Regulation in the Information Age.* MIT Press. ISBN: 9780262018821.

Buragohain, Chiranjeeb, Divyakant Agrawal, and Subhash Suri (2003). “A game theoretic framework for incentives in P2P systems”. In: *Peer-to-Peer Computing, 2003. (P2P 2003). Proceedings. Third International Conference on*, pp. 48–56.

Bygrave, Lee A. (2010). “Privacy and data protection in an international perspective”. In: *Scandinavian studies in law* 56, pp. 165–200.

Canny, John (2002). “Collaborative Filtering with Privacy”. In: *Proceedings of the IEEE Symposium on Security and Privacy.* URL: `http://ieeexplore.ieee.org/xpls/abs%5C_all.jsp?arnumber=1004361`.

Cavoukian, Ann (2009). *Privacy by Design: The 7 Foundational Principles.* URL: http://www.ipc.on.ca/images/resources/7foundationalprinciples.pdf.

Chapman, David and Ajay Jain (1994). *Musk (Version 2) Data Set.* URL: https://archive.ics.uci.edu/ml/datasets/Musk+(Version+2).

Chaum, David L. (1981). "Untraceable electronic mail, return addresses, and digital pseudonyms". In: *Communications of the ACM* 24.2, pp. 84–90.

— (1985). "Security without identification: Transaction systems to make big brother obsolete". In: *Communications of the ACM* 28.10, pp. 1030–1044. URL: http://dl.acm.org/citation.cfm?id=4372.4373.

— (1988). "The dining cryptographers problem: Unconditional sender and recipient untraceability". In: *Journal of cryptology.*

Chawla, Shuchi et al. (2005). "Toward Privacy in Public Databases". In: *Theory of Cryptography.*

Chen, Harry, Tim Finin, and Anupam Joshi (2003). "An ontology for context-aware pervasive computing environments". In: *The Knowledge Engineering Review* 18.3, pp. 197–207.

— (2004). "An Intelligent Broker Architecture for Pervasive Context-Aware Systems". In: *Adjunct proceedings of Ubicomp*, pp. 183–184.

Chen, Rui et al. (2011). "Publishing set-valued data via differential privacy". In: *Proceedings of the VLDB Endowment* 4.11, pp. 1087–1098.

Chor, Benny et al. (1998). "Private information retrieval". In: *Journal of the ACM (JACM)* 45.6, pp. 965–981.

Clarke, Ian et al. (2001). "Freenet: A distributed anonymous information storage and retrieval system". In: *Designing Privacy Enhancing Technologies.* Springer Berlin Heidelberg, pp. 46–66.

Clau*β*, Sebastian, Dogan Kesdogan, and Tobias Kölsch (2005). "Privacy enhancing identity management: protection against re-identification and profiling". In: *Proceedings of the 2005 workshop on Digital identity management.* ACM, pp. 84–93.

Cooper, David et al. (2008). *RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.* URL: http://tools.ietf.org/html/rfc5280.

Cranor, Lorrie Faith, Serge Egelman, et al. (2008). "P3P deployment on websites". In: *Electronic Commerce Research and Applications* 7.3, pp. 274–293.

Cranor, Lorrie Faith, Marc Langheinrich, et al. (2002). *The Platform for Privacy Preferences 1.0 (P3P1.0) Specification.* Tech. rep. W3C. URL: http://www.w3.org/TR/P3P/.

Dalenius, T and SP Reiss (1982). "Data-swapping: A technique for disclosure control". In: *Journal of statistical planning and inference.*

Davies, Nigel and Marc Langheinrich (2013). "Privacy By Design". In: *Pervasive Computing, IEEE* 12.2, pp. 2–4.

Dey, Anind K., Gregory D. Abowd, and Daniel Salber (2001). "A conceptual framework and a toolkit for supporting the rapid prototyping of context-aware applications". In: *Human-Computer Interaction* 16.2, pp. 97–166.

Dierks, Tim and Eric Rescorla (2008). *RFC 5246: The transport layer security (TLS) protocol version 1.2.* URL: http://tools.ietf.org/html/rfc5246.

Dingledine, Roger, Michael J. Freedman, and David Molnar (2001). "The Free Haven Project: Distributed Anonymous Storage Service". In: *Designing Privacy Enhancing Technologies.* Springer Berlin Heidelberg, pp. 67–95.

Dingledine, Roger, Nick Mathewson, and Paul Syverson (2004). *Tor: The second-generation onion router*. Tech. rep. Naval Research Lab. URL: `http://oai.dtic.mil/oai/oai?verb=getRecord%5C&amp;metadataPrefix=html%5C&amp;identifier=ADA465464`.

Domingo-Ferrer, Josep (2011). "Coprivacy: towards a theory of sustainable privacy". In: *Privacy in Statistical Databases*. Springer Berlin Heidelberg.

Doolin, Kevin (2013). *SOCIETIES completes Enterprise User Trial*. URL: `http://www.ict-societies.eu/2013/04/23/societies-completes-enterprise-user-trial/`.

Doolin, Kevin et al. (2012). "SOCIETIES: Where Pervasive Meets Social". In: *The Future Internet Assembly*, pp. 30–41. URL: `http://link.springer.com/chapter/10.1007/978-3-642-30241-1%5C_4`.

Douceur, John (2002). "The Sybil Attack". In: *Peer-to-Peer Systems*. Ed. by Peter Druschel, Frans Kaashoek, and Antony Rowstron. Vol. 2429. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 251–260. ISBN: 978-3-540-44179-3. DOI: `10.1007/3-540-45748-8`.

Du, Wenliang and Mikhail J Atallah (2001). "Secure multi-party computation problems and their applications: a review and open problems". In: *Proceedings of the 2001 workshop on New security paradigms*. ACM, pp. 13–22.

Dwork, Cynthia (2006). "Differential privacy". In: *Automata, languages and programming*, pp. 1–12.

— (2008). "Differential privacy: A survey of results". In: *Theory and Applications of Models of Computation*, pp. 1–19.

— (2011). "A firm foundation for private data analysis". In: *Communications of the ACM* 54.1, pp. 86–95. URL: `http://dl.acm.org/citation.cfm?id=1866758`.

Eckersley, Peter (2010). "How unique is your web browser?" In: *Privacy Enhancing Technologies*. Springer Berlin Heidelberg, pp. 1–18.

Eclipse (2011). *Virgo*. URL: `http://www.eclipse.org/virgo/`.

Eclipse Foundation (2009). *Higgins Personal Data Service*. URL: `http://www.eclipse.org/higgins/`.

Electronic Privacy Information Center (2000). *Pretty Poor Privacy: An Assessment of P3P and Internet Privacy*. URL: `http://epic.org/reports/prettypoorprivacy.html`.

Ellison, Carl and Bruce Schneier (2000). "Ten risks of PKI: What you're not being told about public key infrastructure". In: *Computer Security Journal* 16.1.

Esguerra, Richard (2009). *Google CEO Eric Schmidt Dismisses the Importance of Privacy*. URL: `https://www.eff.org/deeplinks/2009/12/google-ceo-eric-schmidt-dismisses-privacy`.

European Commission (2010). *A Digital Agenda for Europe*. URL: `http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF`.

European Data Protection Supervisor (2013). *Additional EDPS Comments on the Data Protection Reform Package*. URL: `http://www.statewatch.org/news/2013/mar/eu-edps-add-cooments-new-dp-reg.pdf`.

European Telecommunications Standards Institute (2011). "ETSI TS 102 690: Machine-to-Machine communications (M2M); Functional architecture". URL: `http://www.etsi.org/deliver/etsi%5C_ts/102600%5C_102699/102690/01.02.01%5C_60/ts%5C_102690v010201p.pdf`.

Facebook Inc. (2013). *Facebook Reports Fourth Quarter and Full Year 2012 Results*. URL: `http://investor.fb.com/releasedetail.cfm?ReleaseID=736911`.

Federal Trade Commission (2000). *Fair Information Practice Principles.* en. URL: http://www.ftc.gov/reports/privacy3/fairinfo.shtm.

— (2010). *Closing Letter to Reed Freeman, Esq., Counsel for Netflix, Inc.* Tech. rep. Federal Trade Commission. URL: ttp://www.ftc.gov/os/closings/100312netflixletter.pdf.

— (2011). *40 Years of Experience with the Fair Credit Reporting Act: An FTC Staff Report with Summary of Interpretations.* URL: http://www.ftc.gov/os/2011/07/110720fcrareport.pdf.

— (2012). *Protecting consumer privacy in an era of rapid change: Recommendations for businesses and policymakers.* URL: http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

Feldman, Ariel J. et al. (2010). "SPORC: Group Collaboration using Untrusted Cloud Resources." In: *OSDI.*

Fienberg, SE and J McIntyre (2004). "Data swapping: Variations on a theme by dalenius and reiss". In: *Privacy in statistical databases.*

Floréen, Patrik et al. (2005). "Towards a context management framework for MobiLife". In: *Proceedings of the 14th IST Mobile & Communications Summit.*

Fontaine, Caroline and Fabien Galand (2007). "A survey of homomorphic encryption for nonspecialists". In: *EURASIP Journal on Information Security* 2007, p. 15.

Fontanella-Khan, James (2013). *Victory for tech giants on EU data laws.* URL: http://www.ft.com/cms/s/0/5ad18e46-3d8c-11e3-9928-00144feab7de.html.

FreeNet Project (2013). *Freenet REference Daemon - Trunk.* URL: https://github.com/freenet/fred-staging.

Freier, A., P. Karlton, and P. Kocher (1996). "The SSL 3.0 Protocol".

Fung, Benjamin et al. (2010). "Privacy-Preserving Data Publishing: A Survey on Recent Developments". In: *ACM Computing Surveys (CSUR).*

Gallagher, Niall (2006). *Simple XML Serialization.* URL: http://simple.sourceforge.net/.

Garfinkel, S.L., A. Juels, and R. Pappu (2005). "RFID Privacy: An Overview of Problems and Proposed Solutions". In: *IEEE Security and Privacy Magazine* 3.3, pp. 34–43. ISSN: 1540-7993. DOI: 10.1109/MSP.2005.78.

Garfinkel, Tal et al. (2003). "Terra: A virtual machine-based platform for trusted computing". In: *ACM SIGOPS Operating Systems Review* 37.5, pp. 193–206.

Gellman, Robert (2013). *Fair Information Practices: A Basic History.* Tech. rep.

General Secretariat of the European Council (2013). *European Council 24/25 October 2013 - Conclusions.* URL: http://www.consilium.europa.eu/uedocs/cms%5C_data/docs/pressdata/en/ec/139197.pdf.

Gentry, Craig et al. (2009). "Fully homomorphic encryption using ideal lattices". In: *STOC.* Vol. 9, pp. 169–178.

Gentry, Craig and Shai Halevi (2011). "Implementing Gentry's fully-homomorphic encryption scheme". In: *Advances in Cryptology–EUROCRYPT 2011.* Springer, pp. 129–148.

Ghinita, Gabriel, Yufei Tao, and Panos Kalnis (2008). "On the Anonymization of Sparse High-Dimensional Data". In: *IEEE 24th International Conference on Data Engineering.*

Girão, João and Amardeo Sarma (2009). "Identities in the future internet of things". In: *Wireless Personal Communications* 49.3, pp. 353–363. DOI: 10.1007/s11277-009-9697-0.

Girão, João, Amardeo Sarma, and Rui L. Aguiar (2006). "Virtual identities - A cross layer approach to identity and identity management". In: *Proc. 17th Wireless World Research Forum*.

Gkoulalas-Divanis, Aris and Grigorios Loukides (2012). "Utility-guided Clustering-based Transaction Data Anonymization." In: *Transactions on Data Privacy* 5, pp. 223–251. URL: `http://www.tdp.cat/issues11/tdp.a083a11.pdf`.

Glater, Jonathan D. (2006). *Privacy for People Who Don't Show Their Navels*. URL: `http://www.nytimes.com/2006/01/25/technology/techspecial2/25privacy.html`.

Goldberg, Ian (2003). "Privacy-enhancing technologies for the Internet, II: Five years later". In: *Privacy Enhancing Technologies*. Ed. by Roger Dingledine and Paul Syverson. Springer Berlin Heidelberg, pp. 1–12. ISBN: 978-3-540-00565-0. DOI: `10.1007/3-540-36467-6\_1`. URL: `http://link.springer.com/chapter/10.1007/3-540-36467-6%5C_1`.

— (2007). "Privacy enhancing technologies for the Internet III: Ten years later". In: *Digital Privacy: Theory, Technologies, and Practices*.

Goldberg, Ian, David Wagner, and Eric Brewer (1997). "Privacy-enhancing technologies for the Internet". In: *COMPCON '97 Proceedings of the 42nd IEEE International Computer*.

Goldreich, Oded, Silvio Micali, and Avi Wigderson (1987). "How to play any mental game". In: *Proceedings of the nineteenth annual ACM symposium on Theory of computing*. ACM, pp. 218–229.

Goldschlag, David, Michael Reed, and Paul Syverson (1996). "Hiding routing information". In: *Information Hiding*. Springer Berlin Heidelberg, pp. 137–150. DOI: `10.1007/3-540-61996-8\_37`. URL: `http://link.springer.com/chapter/10.1007/3-540-61996-8%5C_37`.

— (1999). "Onion routing". In: *Communications of the ACM* 42.2, pp. 39–41. DOI: `10.1145/293411.293443`.

Gomes, Diogo et al. (2010). "XMPP based Context Management Architecture". In: *2010 IEEE Globecom Workshops*. IEEE, pp. 1372–1377. ISBN: 978-1-4244-8863-6. DOI: `10.1109/GLOCOMW.2010.5700163`.

Gonçalves, João M. (2014). *New York Times Privacy Tag Graph*. URL: `http://jmgoncalv.es/nyt-privacy-tag-graph/`.

— (2015). *New York Times Privacy Tag Timeline*. URL: `http://jmgoncalv.es/nyt-privacy-tag-timeline/`.

Gonçalves, João M., Dirk Delahaye, and Lamorte Lamorte (2010). "Professional and User-Generated Content Rating using Context Information". In: *Networked & Electronic Media Summit 2010*. URL: `http://nem-summit.eu/wp-content/plugins/alcyonis-event-agenda/files/Professional-and-User-Generated-Content-Rating-using-Context-Information.pdf`.

Gonçalves, João M. and Diogo Gomes (2014). "User-Hosted SOA Infrastructure over XMPP". In: *IEEE Symposium on Computers and Communications*. Ed. by IEEE. DOI: `10.1109/ISCC.2014.6912538`.

Gonçalves, João M., Diogo Gomes, and Rui L. Aguiar (2012). "Low-latency privacy-enabled Context Distribution Architecture". In: *Communications (ICC), 2012 IEEE International Conference on*. Ed. by IEEE. Ottawa, pp. 1917–1922. DOI: `10.1109/ICC.2012.6364027`.

Google Inc. (2013a). *Google Earnings Q4 2012*. URL: `http://investor.google.com/earnings/2012/Q4%5C_google%5C_earnings%5C_tab7.html`.

— (2013b). *Using OAuth 2.0 for Login - Google Accounts Authentication and Authorization*. URL: `https://developers.google.com/accounts/docs/OAuth2Login`.

Greenberg, Andy (2013). *Introducing SafeSource, A New Way To Send Forbes Anonymous Tips And Documents.* URL: http://www.forbes.com/sites/andygreenberg/2013/10/29/introducing-safesource-a-new-way-to-send-forbes-anonymous-tips-and-documents/.

Greenleaf, Graham (2012). "Global Data Privacy in a Networked World". In: *Research Handbook on Governance of the Internet.* Ed. by Ian Brown. Edward Elgar. URL: http://papers.ssrn.com/sol3/papers.cfm?abstract%5C_id=1954296.

Greenstein, B, Damon McCoy, and J Pang (2008). "Improving wireless privacy with an identifier-free link layer protocol". In: *Proceedings of the 6th ...*

Greenwald, Glenn (2013). *NSA collecting phone records of millions of Verizon customers daily.* URL: http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

Greenwald, Glenn and Germán Aranda (2013). *La NSA espió 60 millones de llamadas en España en sólo un mes.* URL: http://www.elmundo.es/espana/2013/10/28/526dcbad61fd3d07678b456b.html.

Grosse, E and M Upadhyay (2013). "Authentication at scale". In: URL: http://ieeexplore.ieee.org/xpls/abs%5C_all.jsp?arnumber=6381399.

Grossklags, Jens and Alessandro Acquisti (2007). "When 25 cents is too much: An experiment on willingness-to-sell and willingness-to-protect personal information". In: *Workshop on the Economics of Information Security.*

GroupLens (1997). *MovieLens: movie recommendations.* URL: http://movielens.umn.edu/login.

— (2011). *MovieLens Data Sets.* URL: http://www.grouplens.org/node/73.

Gruteser, Marco and Dirk Grunwald (2003). "Anonymous usage of location-based services through spatial and temporal cloaking". In: *Proceedings of the 1st international conference on Mobile systems, applications and services.*

— (2005). "Enhancing location privacy in wireless LAN through disposable interface identifiers: a quantitative analysis". In: *Mobile Networks and Applications.*

Gu, Tao, Hung Keng Pung, and Da Quing Zhang (2004). "Toward an OSGi-based infrastructure for context-aware applications". In: *Pervasive Computing, IEEE* 3.4, pp. 66–74.

Gunawardana, Asela and Guy Shani (2009). "A survey of accuracy evaluation metrics of recommendation tasks". In: *The Journal of Machine Learning Research* 10, pp. 2935–2962. URL: http://dl.acm.org/citation.cfm?id=1755883.

Gürses, Seda, Carmela Troncoso, and Claudia Diaz (2011). "Engineering privacy by design". In: *Computers, Privacy & Data Protection.*

Gustavsen, Richard Moe (2002). "Condor–an application framework for mobility-based context-aware applications". In: *Proceedings of the workshop on concepts and models for ubiquitous computing.*

Hachamovitch, Dean (2012). *Google Bypassing User Privacy Settings.*

Halderman, J. Alex et al. (2009). "Lest We Remember: Cold Boot Attacks on Encryption Keys". In: *Communications of the ACM* 52.5, pp. 91–98.

Hammer, Eran (2012). *OAuth 2.0 and the Road to Hell.* URL: http://hueniverse.com/2012/07/oauth-2-0-and-the-road-to-hell/.

Hammer-Lahav, Eran (2010). *RFC 5849: The OAuth 1.0 Protocol.* URL: http://tools.ietf.org/html/rfc5849.

Hampton, Keith N. et al. (2011). *Social networking sites and our lives.* Tech. rep. Pew Research Center. URL: http://pewinternet.org/Reports/2011/Technology-and-social-networks.aspx.

Hansen, Marit et al. (2004). "Privacy-enhancing identity management". In: *Information Security Technical Report* 9.1, pp. 35–44. ISSN: 13634127. DOI: 10.1016/S1363-4127(04)00014-7.

Hapner, Mark et al. (2002). *JSR 914: JavaTM Message Service (JMS) API.* Tech. rep. Java Community Process. URL: http://www.jcp.org/en/jsr/detail?id=914.

Hardt, Dick (2012). *RFC 6749: The OAuth 2.0 Authorization Framework.* URL: http://tools.ietf.org/html/rfc6749.

Harper, Jim (2005). "Book Review: The Digital Person: Technology and Privacy in the Information Age by Daniel J. Solove". In: *Cato Journal* 25.4, pp. 641–644.

Helft, Miguel and Jenna Wortham (2010). *Facebook Bows to Pressure Over Privacy.* URL: http://www.nytimes.com/2010/05/27/technology/27facebook.html.

Herley, Cormac (2012). "Why do nigerian scammers say they are from nigeria?" In: *Workshop on the Economics of Information Security.* URL: ftp://ftp.fixme.ch/free%5C_for%5C_all/Ebook/Nigerian%5C_Scammers.pdf.

Hickman, Kipp (1995). "The SSL Protocol".

Hofer, Thomas et al. (2003). "Context-awareness on mobile devices-the hydrogen approach". In: *Proceedings of the 36th Annual Hawaii International Conference on System Sciences.*

Hong, Jason and James Landay (2001). "An infrastructure approach to context-aware computing". In: *Human-Computer Interaction* 16.2, pp. 287–303.

Hoonakker, P, N Bornoe, and P Carayon (2009). "Password authentication from a human factors perspective: Results of a survey among end-users". In: *Proceedings of the Human . . .*

Huang, Leping, Kanta Matsuura, et al. (2005). "Enhancing wireless location privacy using silent period". In: *Wireless Communications and Networking Conference, 2005 IEEE.* DOI: 10.1109/WCNC.2005.1424677.

Huang, Leping, Hiroshi Yamane, et al. (2006). "Towards modeling wireless location privacy". In: *Privacy Enhancing Technologies.* Springer Berlin Heidelberg, pp. 59–77. DOI: 10.1007/11767831_5.

Hughes, Eric (1993). *A Cypherpunk's Manifesto.* URL: http://w2.eff.org/Privacy/Crypto/Crypto%5C_misc/cypherpunk.manifesto.

Ignite Realtime (2002a). *Openfire.* URL: http://www.igniterealtime.org/projects/openfire/.

— (2002b). *Smack.* URL: http://www.igniterealtime.org/projects/smack/index.jsp.

— (2002c). *Whack.* URL: http://www.igniterealtime.org/projects/whack/index.jsp.

Inkster, Toby, Henry Story, and Bruno Harbulot (2014). *WebID Authentication over TLS.* Tech. rep. URL: http://www.w3.org/2005/Incubator/webid/spec/tls/.

Java.net (2003). *Java Architecture for XML Binding (JAXB).* URL: https://jaxb.java.net/.

Jensen, Carlos and Colin Potts (2003). *Private Policies Examined: Fair Warning or Fair Game?* URL: http://smartech.gatech.edu/handle/1853/3215.

John, Leslie K., Alessandro Acquisti, and George Loewenstein (2009). "The best of strangers: Context dependent willingness to divulge personal information". URL: http://papers.ssrn.com/sol3/papers.cfm?abstract%5C_id=1430482.

Kadri, Saqib (2008). *Kadri Framework C++ Source Code (Pre-Processing, Dates, Blending)*. URL: http://www.netflixprize.com/community/viewtopic.php?pid=9202.

Kalatzis, Nikos et al. (2013). "Cross-community context management in Cooperating Smart Spaces". In: *Personal and Ubiquitous …* 779, pp. 1–17. URL: http://link.springer.com/article/10.1007/s00779-013-0654-2.

Kerr, Ian, Valerie Steeves, and Carole Lucock (2009). *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*. Oxford University Press, USA. ISBN: 0195372476. URL: http://www.idtrail.org/content/view/799.

Koblitz, Neal (1987). "Elliptic curve cryptosystems". In: *Mathematics of computation* 48.177, pp. 203–209.

Koblitz, Neal, Alfred Menezes, and Scott Vanstone (2000). "The state of elliptic curve cryptography". In: *Towards a Quarter-Century of Public Key Cryptography*, pp. 103–123.

Kosinski, Robert J. (2008). "A literature review on reaction time". In: *Clemson University*. URL: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/biae.clemson.edu/bpc/bp/Lab/110/reaction.htm.

Krebs, Brian (2013). *Experian Sold Consumer Data to ID Theft Service*. URL: http://krebsonsecurity.com/2013/10/experian-sold-consumer-data-to-id-theft-service/.

Kroes, Neelie (2010). *Towards more confidence and more value for European Digital Citizens*. URL: http://europa.eu/rapid/press-release%5C_SPEECH-10-452%5C_en.htm.

Kushilevitz, Eyal and Rafail Ostrovsky (1997). "Replication is not needed: Single database, computationally-private information retrieval". In: *focs*. IEEE, p. 364.

La Quadrature du Net (2013). *Major Loopholes in Privacy Regulation - EU Parliament Must Stand For Citizens*. URL: http://www.laquadrature.net/en/major-loopholes-in-privacy-regulation-eu-parliament-must-stand-for-citizens.

Langheinrich, Marc (2001). "Privacy by design—principles of privacy-aware ubiquitous systems". In: *Ubicomp 2001: Ubiquitous Computing*. Springer Berlin Heidelberg, pp. 273–291. DOI: 10.1007/3-540-45427-6_23.

— (2009). "A survey of RFID privacy approaches". In: *Personal and Ubiquitous Computing* 13.6, pp. 413–421.

Leavitt, Neal (2011). "Internet security under attack: The undermining of digital certificates". In: *Computer* 44.12, pp. 17–20.

Lederer, S. et al. (2004). "Personal privacy through understanding and action: five pitfalls for designers". In: *Personal and Ubiquitous Computing* 8.6, pp. 440–454.

Leon, Pedro Giovanni et al. (2010). "Token attempt: the misrepresentation of website privacy policies through the misuse of p3p compact policy tokens". In: *ACM Workshop on Privacy in the Electronic Society (WPES 2010)*, pp. 93–104.

Li, Ninghui, Tiancheng Li, and Suresh Venkatasubramanian (2007). "t-closeness: Privacy beyond k-anonymity and l-diversity". In: *IEEE 23rd International Conference on Data Engineering*.

Li, Tiancheng et al. (2012). "Slicing: A New Approach for Privacy Preserving Data Publishing". In: *IEEE Transactions on Knowledge and Data Engineering* 24.3, pp. 561–574.

Liu, Hui et al. (2007). "Survey of Wireless Indoor Positioning Techniques and Systems". In: *IEEE Transactions on Systems, Man and Cybernetics, Part C (Applications and Reviews)* 37.6, pp. 1067–1080. ISSN: 1094-6977.

Liu, Y and KP Gummadi (2011). “Analyzing Facebook privacy settings: User expectations vs. reality”. In: *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference*, pp. 61–70.

Ludwig, Scott et al. (2009). *XEP-0166: Jingle.* Tech. rep. XMPP Standards Foundation. URL: http://xmpp.org/extensions/xep-0166.html.

Macaskill, Ewen and Gabriel Dance (2013). *NSA Files: Decoded - What the revelations mean for you.* URL: http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded.

Machanavajjhala, Ashwin et al. (2007). “l-diversity: Privacy beyond k-anonymity”. In: *ACM Transactions on Knowledge Discovery from Data (TKDD)* 1.1, p. 3.

Madden, Mary et al. (2013). *Teens, Social Media, and Privacy.* Tech. rep. Pew Research Center. URL: http://pewinternet.org/Reports/2013/Teens-Social-Media-And-Privacy.aspx.

Maier, Fran (2010). *More on The Problem with P3P.* URL: http://www.truste.com/blog/2010/09/14/more-on-the-problem-with-p3p/.

Maler, E (2003). *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML).* URL: https://www.oasis-open.org/committees/security/docs/draft-sstc-core-28.pdf.

Maler, Eve and Drummond Reed (2008). “The venn of identity: Options and issues in federated identity management”. In: *IEEE Security & Privacy* 2, pp. 16–23.

Martucci, Leonardo A., Sebastian Ries, and Max Mühlhäuser (2011). “Sybil-free pseudonyms, privacy and trust: Identity management in the internet of services”. In: *Journal of Information Processing* 19, pp. 317–331.

Marx, Gary T. (2001). “Murky conceptual waters: The public and the private”. In: *Ethics and Information Technology* 3.3, pp. 157–169.

Mason, Rowena (2009). *Acxiom: the company that knows if you own a cat or if you’re right-handed.* URL: http://www.telegraph.co.uk/finance/newsbysector/retailandconsumer/5231752/Acxiom-the-company-that-knows-if-you-own-a-cat-or-if-youre-right-handed.html.

Matos, Alfredo (2012). “Privacy in Next Generation Networks”. PhD thesis. Universidade de Aveiro.

Matos, Alfredo, João Girão, et al. (2007). “Preserving privacy in mobile environments with virtual network stacks”. In: *IEEE Global Telecommunications Conference (GLOBECOM) 2007.*

Matos, Alfredo, Susana Sargento, and Rui L. Aguiar (2007). “Embedding identity in mobile environments”. In: *Proceedings of 2nd ACM/IEEE international workshop on Mobility in the evolving internet architecture.* URL: http://dl.acm.org/citation.cfm?id=1366927.

Mayer, Jonathan (2012). *Safari Trackers.* URL: http://webpolicy.org/2012/02/17/safari-trackers/.

Mayer, Jonathan and Arvind Narayanan (2013). *Do Not Track: Implementations.* URL: http://www.donottrack.us/implementations.

Mayer, Jonathan, Arvind Narayanan, and Sid Stamm (2011). *Do Not Track: A Universal Third-Party Web Tracking Opt Out.* URL: http://tools.ietf.org/html/draft-mayer-do-not-track-00.

McDonald, Aleecia M. and Lorrie Faith Cranor (2008). “The Cost of Reading Privacy Policies”. In: *ISJLP* 4.

— (2010). “Beliefs and Behaviors: Internet Users’ Understanding of Behavioral Advertising”. In: *TPRC 2010: The 38th Research Conference on Communication, Information and Internet Policy.*

McSherry, Frank and Ilya Mironov (2009). “Differentially private recommender systems: building privacy into the net”. In: *15th ACM International Conference on Knowledge Discovery and Data Mining (ACM SIGKDD)*, pp. 627–636.

Mead, G H (1934). *Mind, Self and Society*. Ed. by Charles W Morris. Vol. 1. 10. University of Chicago Press, pp. 1–264. ISBN: 0226516687. DOI: 10.1037/h0053424. URL: http://www.sciencedirect.com/science/article/B6WY5-4NSXCJW-C/2/7b6406086572f41f421a3a80172469d8.

Merener, Martin M. (2012). “Theoretical results on de-anonymization via linkage attacks”. In: *Transactions on Data Privacy* 5, pp. 377–402. URL: http://dl.acm.org/citation.cfm?id=2423652.

Meyer, Benjamin (2006). *Netflix Recommender Framework*. URL: http://www.netflixprize.com/community/viewtopic.php?id=352.

Meyerson, Adam and Ryan Williams (2004). “On the complexity of optimal k-anonymity”. In: *Proceedings of the twenty-third ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems*, pp. 223–228. URL: http://dl.acm.org/citation.cfm?id=1055591.

Millard, Peter, Peter Saint-Andre, and Ralph Meijer (2010). *XEP-0060: Publish-Subscribe*. Tech. rep. XMPP Standards Foundation. URL: http://xmpp.org/extensions/xep-0060.html.

Miller, Claire Cain (2013a). *Lawmakers Show Concerns About Google’s New Glasses*. URL: http://www.nytimes.com/2013/05/17/technology/lawmakers-pose-questions-on-google-glass.html.

— (2013b). *Tech Companies Concede to Surveillance Program*. URL: http://www.nytimes.com/2013/06/08/technology/tech-companies-bristling-concede-to-government-surveillance-efforts.html?pagewanted=all.

Mozilla (2011). *Privacy Icons*. Tech. rep. URL: https://wiki.mozilla.org/Privacy%5C_Icons.

Mozilla Developer Network (2012). *BrowserID Protocol Overview*. URL: https://developer.mozilla.org/en-US/Persona/Protocol_Overview.

Naehrig, Michael, Kristin Lauter, and Vinod Vaikuntanathan (2011). “Can homomorphic encryption be practical?” In: *Proceedings of the 3rd ACM workshop on Cloud computing security workshop*. ACM, pp. 113–124.

Naor, Moni and Kobbi Nissim (2001). “Communication preserving protocols for secure function evaluation”. In: *Proceedings of the thirty-third annual ACM symposium on Theory of computing*. ACM, pp. 590–599.

Narayanan, Arvind and Vitaly Shmatikov (2008). “Robust De-anonymization of Large Sparse Datasets”. In: *IEEE Symposium on Security and Privacy*, pp. 111–125.

— (2010). “Myths and fallacies of personally identifiable information”. In: *Communications of the ACM* 53.6, pp. 24–26.

Nergiz, M. Ercan, Maurizio Atzori, and Christopher W. Clifton (2007). “Hiding the presence of individuals from shared databases”. In: *Proceedings of the 2007 ACM SIGMOD international conference on Management of data*, pp. 665–676.

Netflix (2009). *Grand Prize awarded to team BellKor’s Pragmatic Chaos*. URL: http://www.netflixprize.com/community/viewtopic.php?id=1537.

Norberg, Patricia A., Daniel R. Horne, and David A. Horne (2007). “The privacy paradox: Personal information disclosure intentions versus behaviors”. In: *Journal of Consumer Affairs* 41.1, pp. 100–126.

Olumofin, Femi and Ian Goldberg (2012). “Revisiting the computational practicality of private information retrieval”. In: *Financial Cryptography and Data Security*. Springer, pp. 158–172.

Organisation for Economic Co-operation and Development (1980). *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* Tech. rep. URL: `http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm`.

Osvik, DA, Adi Shamir, and E Tromer (2006). “Cache attacks and countermeasures: the case of AES”. In: *Topics in Cryptology – CT-RSA 2006.* Springer Berlin Heidelberg, pp. 1–26.

Papadopoulou, Elizabeth et al. (2008). “Linking Privacy and User Preferences in the Identity Management for a Pervasive System”. In: *IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology.* IEEE, pp. 192–195. ISBN: 978-0-7695-3496-1. DOI: `10.1109/WIIAT.2008.331`.

Pascoe, Jason (1998). “Adding generic contextual capabilities to wearable computers”. In: *Second International Symposium on Wearable Computers*, pp. 92–99.

Paspallis, Nearchos et al. (2008). “A pluggable and reconfigurable architecture for a context-aware enabling middleware system”. In: *On the Move to Meaningful Internet Systems: OTM 2008*, pp. 553–570.

Pathak, Manas A. and Bhiksha Raj (2011). “Efficient Protocols for Principal Eigenvector Computation over Private Data.” In: *Transactions on Data Privacy* 4, pp. 129–146. URL: `http://www.cs.cmu.edu/afs/cs.cmu.edu/Web/People/manasp/docs/ppsvd-tdp.pdf`.

Pavlou, Paul A. (2011). “State of the information privacy literature: where are we now and where should we go”. In: *MIS Quarterly* 35.4, pp. 977–988.

Perez, Ronald, Reiner Sailer, and Leendert van Doorn (2006). “vTPM: virtualizing the trusted platform module”. In: *Proc. 15th Conf. on USENIX Security Symposium*, pp. 305–320.

Pfitzmann, Andreas and Marit Hansen (2010). *A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management.* Tech. rep. URL: `http://dud.inf.tu-dresden.de/literatur/Anon%5C_Terminology%5C_v0.34.pdf`.

Polat, Huseyin and Wenliang Du (2003). “Privacy-preserving collaborative filtering using randomized perturbation techniques”. In: *Proceedings of the Third IEEE International Conference on Data Mining.* URL: `http://surface.syr.edu/eecs/18/?utm%5C_source=surface.syr.edu/eecs/18%5C&utm%5C_medium=PDF%5C&utm%5C_campaign=PDFCoverPages`.

Poole, Christopher (2010). “The Case for Anonymity Online”. In: *TED2010.* URL: `https://www.ted.com/talks/christopher_m00t_poole_the_case_for_anonymity_online`.

Prekop, Pauk and Mark Burnett (2003). “Activities, context and ubiquitous computing”. In: *Computer Communications* 26.11, pp. 1168–1176.

Privacy Leadership Initiative (2001). *Privacy Notices Research - Final Results.* Tech. rep. URL: `http://www.ftc.gov/bcp/workshops/glb/supporting/harris%20results.pdf`.

Punie, Yves (2003). “A social and technological view of Ambient Intelligence in Everyday Life: What bends the trend?” In: *Key deliverable, The European Media and Technology in Everyday Life Network.*

Rainie, Lee et al. (2013). *Anonymity, Privacy, and Security Online.* Tech. rep. Pew Research Center. URL: `http://pewinternet.org/Reports/2013/Anonymity-online.aspx`.

Rannenberg, Kai (1993). “Recent Development in Information Technology Security Evaluation-The Need for Evaluation Criteria for Multilateral Security.” In: *Security and Control of Information Technology in Society*, pp. 113–128.

— (2000). “Multilateral security a concept and examples for balanced security”. In: *Proceedings of the 2000 New security Paradigms Workshop (NSPW 2000).* ACM, pp. 151–162.

— (2011). “ISO/IEC standardization of identity management and privacy technologies”. In: *Datenschutz und Datensicherheit - DuD* 35.1, pp. 27–29.

Raskin, Aza (2010). *Privacy Icons: Alpha Release.* URL: http://www.azarask.in/blog/post/privacy-icons/.

Raskin, Aza and Arun Ranganathan (2010). “Privacy: A Pictographic Approach”. In: *W3C Workshop on Privacy for Advanced Web APIs.* URL: http://www.w3.org/2010/api-privacy-ws/papers/privacy-ws-22.txt.

Recordon, D and D Reed (2006). “OpenID 2.0: a platform for user-centric identity management”. In: *Proceedings of the second ACM workshop on ...*

Reding, Viviane (2012). *The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age.* URL: http://europa.eu/rapid/press-release%5C_SPEECH-12-26%5C_en.htm.

Reichle, Roland, Michael Wagner, Mohammad Ullah Khan, Kurt Geihs, Jorge Lorenzo, et al. (2008). “A comprehensive context modeling framework for pervasive computing systems”. In: *Distributed Applications and Interoperable Systems.* Springer Berlin Heidelberg, pp. 281–295.

Reichle, Roland, Michael Wagner, Mohammad Ullah Khan, Kurt Geihs, Massimo Valla, et al. (2008). “A Context Query Language for Pervasive Computing Environments”. In: *Sixth Annual IEEE International Conference on Pervasive Computing and Communications*, pp. 434–440.

Remote Storage (2013). *remotestorage.io.* URL: http://remotestorage.io/.

Rivest, Ron L., Adi Shamir, and Leonard Adleman (1978). “A method for obtaining digital signatures and public-key cryptosystems”. In: *Communications of the ACM* 21.2, pp. 120–126.

Román, Manuel et al. (2002). “A Middleware Infrastructure for Active Spaces”. In: *IEEE Pervasive Computing* 1.4, pp. 74–83.

Roy, Jessica (2013). *Everything You Need to Know About Silk Road, the Online Black Market Raided by the FBI.* URL: http://nation.time.com/2013/10/04/a-simple-guide-to-silk-road-the-online-black-market-raided-by-the-fbi/.

Rubinstein, Ira (2012). “Regulating privacy by design”. In: *Berkeley Technology Law Journal* 26, pp. 1409–1456.

Sabo, John et al. (2012). *Privacy Management Reference Model and Methodology (PMRM) Version 1.0.* URL: http://docs.oasis-open.org/pmrm/PMRM/v1.0/csprd01/PMRM-v1.0-csprd01.pdf.

Sadeh, Norman et al. (2009). “Understanding and capturing people’s privacy policies in a mobile social networking application”. In: *Personal and Ubiquitous Computing* 13.6, pp. 401–412.

Sailer, Reiner, Trent Jaeger, et al. (2005). “Building a MAC-based security architecture for the Xen open-source hypervisor”. In: *Computer Security Applications Conference, 21st Annual.*

Sailer, Reiner, Xiaolan Zhang, et al. (2004). “Design and Implementation of a TCG-based Integrity Measurement Architecture.” In: *Proceedings of the 13th conference on USENIX Security Symposium.*

Saint-Andre, Peter et al. (2012). *XEP-0277: Microblogging over XMPP.* Tech. rep. XMPP Standards Foundation. URL: http://xmpp.org/extensions/xep-0277.html.

Samarati, P and Latanya Sweeney (1998). “Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression”. In: URL: http://epic.org/privacy/reidentification/Samarati%5C_Sweeney%5C_paper.pdf.

Schmidt, Howard A. (2011). *Advancing the National Strategy for Trusted Identities in Cyberspace: Government as Early Adopter.* URL: `http://www.whitehouse.gov/blog/2011/10/14/advancing-national-strategy-trusted-identities-cyberspace-government-early-adopter`.

Schneier, Bruce (2006). *The Eternal Value of Privacy.* URL: `http://www.wired.com/politics/security/commentary/securitymatters/2006/05/70886`.

Schonfeld, Erick (2009). *The Online Ad Recession Is Officially Here: First Quarterly Decline In Revenues.* URL: `http://techcrunch.com/2009/05/01/the-online-ad-recession-is-officially-here-first-quarterly-decline-in-revenues/`.

Schwartz, A (2009). "Looking back at P3P: lessons for the future". In: URL: `https://healthprivacy.org/files/pdfs/P3P%5C_Retro%5C_Final%5C_0.pdf`.

Sengupta, Somini (2013). *Staying Private on the New Facebook.* URL: `http://www.nytimes.com/2013/02/07/technology/personaltech/protecting-your-privacy-on-the-new-facebook.html`.

Serjantov, A, Roger Dingledine, and Paul Syverson (2003). "From a trickle to a flood: Active attacks on several mix types". In: *Information Hiding.* URL: `http://link.springer.com/chapter/10.1007/3-540-36415-3%5C_3`.

Shannon, Claude E. (1948). "A Mathematical Theory of Communication". In: *Bell System Technical Journal.* The mathematical theory of communication 27.July 1928, pp. 379–423. ISSN: 15591662. DOI: `10.1145/584091.584093`.

Sheikh, Kamran, Maarten Wegdam, and Marten van Sinderen (2008). "Quality-of-Context and its use for Protecting Privacy in Context Aware Systems". In: *Journal of Software* 3.3, pp. 83–93.

Simões, José et al. (2009). "CATS: Context-Aware Triggering System for Next Generation Networks". In: *IFIP Advances in Information and Communication Technology: Wireless and Mobile Networking.* Ed. by Jozef Wozniak et al. Springer Berlin Heidelberg, pp. 251–262. ISBN: 978-3-642-03840-2. DOI: `10.1007/978-3-642-03841-9\_23`.

Singer, Natasha (2012). *Mapping, and Sharing, the Consumer Genome.* URL: `http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html`.

Sion, Radu and Bogdan Carbunar (2007). "On the computational practicality of private information retrieval". In: *In Proceedings of the Network and Distributed Systems Security Symposium.*

Smith, H. Jeff, Tamara Dinev, and Heng Xu (2011). "Information privacy research: An interdisciplinary review". In: *MIS Quarterly* 35.4, pp. 989–1016.

SOCIETIES (2011). *GitHub: SOCIETIES.* URL: `https://github.com/societies/`.

Soghoian, Christopher (2011a). *The History of the Do Not Track Header.* URL: `http://paranoia.dubfire.net/2011/01/history-of-do-not-track-header.html`.

— (2011b). "Why private browsing modes do not deliver real privacy". URL: `http://files.cloudprivacy.net/private-browsing-position-paper.pdf`.

Solove, Daniel J. (2002). "Conceptualizing Privacy". In: *California Law Review* 90.4, pp. 1087–1155.

— (2004). *The digital person: Technology and privacy in the information age.* NYU Press. ISBN: 9780814740378.

— (2006). "A Taxonomy of Privacy". In: *University of Pennsylvania Law Review* 154.3, pp. 477–560.

— (2007). "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy". In: *San Diego Law Review* 44, pp. 745–772.

Sovis, Pavol, Florian Kohlar, and Jörg Schwenk (2010). "Security Analysis of OpenID". In: *Sicherheit*, pp. 329–340.

Spiekermann, S and Lorrie Faith Cranor (2009). "Engineering privacy". In: *Software Engineering, IEEE Transactions on* 35.1, pp. 67–82.

Starner, Thad (2013). "Project Glass: An Extension of the Self". In: *Pervasive Computing, IEEE* 12.2, pp. 14–16.

Story, Henry et al. (2009). "Foaf+ ssl: Restful authentication for the social web". In: *Proceedings of the First Workshop on Trust and Privacy on the Social and Semantic Web (SPOT2009).*

Streitfeld, David (2013). *Google Glass Picks Up Early Signal: Keep Out.* URL: `http://www.nytimes.com/2013/05/07/technology/personaltech/google-glass-picks-up-early-signal-keep-out.html`.

Su, Xiaoyuan and Taghi M. Khoshgoftaar (2009). "A survey of collaborative filtering techniques". In: *Advances in artificial intelligence* 4. URL: `http://dl.acm.org/citation.cfm?id=1722966`.

Sun. *Sun XACML Implementation.* URL: `http://sunxacml.sourceforge.net/`.

Sun, San-Tsai et al. (2011). "What makes users refuse web single sign-on?: an empirical investigation of OpenID". In: *Proceedings of the Seventh Symposium on Usable Privacy and Security.* ACM, p. 4.

Suther, Tim (2009). *Data... the New Black.* URL: `http://www.slideshare.net/TimSuther/acxiom-high-performance-data-is-the-new-black`.

Sweeney, Latanya (2000). "Simple demographics often identify people uniquely". In: *Health (San Francisco)*, pp. 1–34.

— (2002). "k-anonymity: A model for protecting privacy". In: *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems* 10.05, pp. 557–570.

Teltscher, Susan et al. (2013). *Measuring the Information Society.* Tech. rep. International Telecommunication Union. URL: `http://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2013/MIS2013%5C_without%5C_Annex%5C_4.pdf`.

Tene, Omer and Jules Polenetsky (2012). "To Track or Do Not Track: Advancing Transparency and Individual Control in Online Behavioral Advertising". In: *Minnesota Journal of Law, Science & Technology* 13.1, pp. 281–357.

Terrovitis, M and N Mamoulis (2008). "Privacy preservation in the publication of trajectories". In: *Mobile Data Management, 2008. ...*

Terrovitis, Manolis, Nikos Mamoulis, and Panos Kalnis (2008). "Privacy-preserving anonymization of set-valued data". In: *Proceedings of the VLDB Endowment* 1.1, pp. 115–125.

Terrovitis, Manolis, Nikos Mamoulis, John Liagouris, et al. (2012). "Privacy preservation by disassociation". In: *Proceedings of the VLDB Endowment* 5.10, pp. 944–955.

Thoughtcrime Labs (2011). *Convergence.* URL: `http://convergence.io/`.

Toch, Eran et al. (2009). "Analyzing use of privacy policy attributes in a location sharing application". In: *Proceedings of the 5th ACM Symposium on Usable Privacy and Security.*

Tor Project (2013). *Tor and the Silk Road takedown.* URL: `https://blog.torproject.org/blog/tor-and-silk-road-takedown`.

Toubiana, Vincent et al. (2010). "Adnostic: Privacy Preserving Targeted Advertising." In: *NDSS Symposium.*

Tsai, Janice Y. et al. (2010). “Location-sharing technologies: Privacy risks and controls”. In: *ISJLP* 6, pp. 119–317.

Turow, Joseph (2003). *Americans and Online Privacy - The System is Broken*. Tech. rep. Annenberg Public Policy Center. URL: http://www.annenbergpublicpolicycenter.org/Downloads/Information%5C_And%5C_Society/20030701%5C_America%5C_and%5C_Online%5C_Privacy/20030701%5C_online%5C_privacy%5C_report.pdf.

Twitter Inc. (2013). *Form S-1, IPO Prospectus*. Tech. rep. United States Securities and Exchange Commission. URL: http://www.sec.gov/Archives/edgar/data/1418091/000119312513390321/d564001ds1.htm.

Vardjan, Mitja and Jan Porekar (2013). “Privacy Monitoring and Assessment for Ubiquitous Systems”. In: *The Fifth International Conferences on Advanced Service Computing*.

Waher, Peter (2013). *XEP-0323: Internet of Things - Sensor Data*. Tech. rep. XMPP Standards Foundation. URL: http://xmpp.org/extensions/xep-0323.html.

Ware, Henry and Fabian Frédérick. *vmstat*. URL: http://linux.die.net/man/8/vmstat.

Ware, Willis H. (1973). *Records, Computers and the Rights of Citizens*. Tech. rep. URL: http://www.rand.org/pubs/papers/P5077.html.

Warren, Samuel D. and Louis D. Brandeis (1890). “The Right to Privacy”. In: *Harvard Law Review* 4.5, pp. 193–220.

Wellerstein, Alex (2013). *Science and Democracy Network Images*. URL: http://www.hks.harvard.edu/sdn/sdnimages/.

Wendlandt, Dan, David G. Andersen, and Adrian Perrig (2008). “Perspectives: Improving SSH-style Host Authentication with Multi-Path Probing”. In: *USENIX Annual Technical Conference*. Vol. 8, pp. 321–334.

Westin, Alan F. (1968). “Privacy and Freedom”. In: *Washington and Lee Law Review* 25.1.

Westin, Alan F. and Michael A. Baker (1972). *Databanks in a free society: computers, record-keeping, and privacy*. Quadrangle Books. ISBN: 9780812902921.

Wiggs, Lance (2010). *The Grandmother effect is starting for Facebook*. URL: http://lancewiggs.com/2010/02/15/the-grandmother-effect-is-starting-for-facebook/.

Winograd, Terry (2001). “Architectures for context”. In: *Human-Computer Interaction* 16.2, pp. 401–419.

Wishart, Ryan, Karen Henricksen, and Jadwiga Indulska (2007). “Context privacy and obfuscation supported by dynamic context source discovery and processing in a context management system”. In: *Ubiquitous Intelligence and Computing*. Springer Berlin Heidelberg, pp. 929–940.

Wu, Geng et al. (2011). “M2M: From mobile to embedded internet”. In: *Communications Magazine, IEEE* 49.4, pp. 36–43.

Xu, Yabo et al. (2008). “Publishing Sensitive Transactions for Itemset Utility”. In: *IEEE 8th International Conference on Data Mining*.

Xu, Yabu et al. (2008). “Anonymizing Transaction Databases for Publication”. In: *Proceedings of the 14th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*.

Yao, Andrew Chi-Chih (1982). “Protocols for secure computations”. In: *FOCS*. Vol. 82, pp. 160–164.

Yekhanin, Sergey (2010). “Private information retrieval”. In: *Communications of the ACM* 53.4, pp. 68–73.

Ylonen, Tatu and Chris Lonvick (2006). *RFC 4251: The Secure Shell (SSH) Protocol Architecture.* URL: `http://tools.ietf.org/html/rfc4251`.

Zafar, Madiha et al. (2009). "Context Management Architecture for Future Internet Services". In: *ICT Mobile Summit 2009.*

Zakerzadeh, Hessam, Char Aggarwal, and Ken Barker (2014). "Towards Breaking the Curse of Dimensionality for High-Dimensional Privacy". In: *SIAM International Conference on Data Mining (SDM).*

Zhan, Justin et al. (2010). "Privacy-preserving collaborative recommender systems". In: *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews* 40.4, pp. 472–476. URL: `http://ieeexplore.ieee.org/xpls/abs%5C_all.jsp?arnumber=5411745`.