Digital Enlightenment Yearbook 2013
M. Hildebrandt et al. (Eds.)
IOS Press, 2013

doi:10.3233/978-1-61499-295-0-102

Personal Information Markets and Privacy: A New Model to Solve the Controversy[1]

Alexander NOVOTNY[2] and Sarah SPIEKERMANN
Vienna University of Economics and Business

Abstract. From the earliest days of the information economy, personal data has been its most valuable asset. Despite data protection laws, companies trade personal information and often intrude on the privacy of individuals. As a result, consumers feel that they do not have control, and lose trust in electronic environments. Technologists and regulators are struggling to develop solutions that meet the demands of business for more personal information while maintaining privacy. However, no promising proposals seem to be in sight. We propose a 3-tier personal information market model with privacy. In our model, clear roles, rights and obligations for all actors re-establish trust. The 'relationship space' enables data subjects and visible business partners to build trusting relationships. The 'service space' supports customer relationships with distributed information processing. The 'rich information space' enables anonymized information exchange. To transition to this model, we show how existing privacy-enhancing technologies and legal requirements can be integrated.

Keywords. Informational privacy, personal data markets, privacy regulation

Introduction

The digital economy is faced with a dilemma. From its inception, personal information (PI) has emerged as the digital economy's core asset. PI is "any information relating to an *identified or identifiable* natural person" [1]. Abundantly leveraged as a free commons, PI is at the core of the Internet economy and is considered the motor for online innovation. "Personal data is the new oil of the Internet and the new currency of the digital world" [2]. It finances the Internet's free content. It strengthens an Internet company's competitive stance. In cases such as social networking it is actually the key ingredient that brings an online service to life.

Besides playing a key economic role, PI is associated with many people's notion of humanity: identity, dignity and privacy. And as PI is increasingly collected, used, packaged, and sold, more conflict arises around how people can retain control of their identities and protect their dignity and privacy. Under the umbrella terms "data protection" and "privacy" – the ability to control both the circulation of PI (out-flowing information) and the access of others to the self (in-flowing information) [3] – a global political debate has emerged. This debate centers on whether people should be enabled to control their PI and which aspects companies should be allowed to use.

[1] An earlier, short version of this essay was published in Alt, R., Franczyk, B. (eds.): Proceedings of the 11th International Conference on Wirtschaftsinformatik, Feb 27th–Mar 01st, pp. 1635–1649, Leipzig, Germany (2013).

[2] Corresponding Author.

In the meantime, the economic realities of personal data markets on one side and data protection efforts on the other are drifting apart. Companies capitalize on opportunities to collect and trade PI on an unprecedented scale. Uncontrolled PI trading has evolved [4]. Every time a user surfs online, an average of 56 parties track their activities on a website, largely without their consent or knowledge [5]. Companies claim 'legitimate' business interests in the data they collect. They argue that individuals and companies benefit equally, and that, in any case, the data belongs to the companies. It is estimated that at least 1,200 companies currently profile people for advertisements and marketing [6]. The digital marketing association claims that "marketing fuels the world" [7], profiling is enabling more relevant ads and serving as the only way for companies to provide free online services and content. Device manufacturers assert that they benefit end users by regularly uploading a myriad of information about hardware usage patterns, thereby increasing product quality [8]. And because companies have created these records, they believe that they own the data [9]. As a result, companies treat the use of PI as an issue of self-regulation. Major self-regulatory efforts, though, such as the Safe Harbor Agreement and the "do not track" initiatives, are failing [7].

Against this background, regulators, privacy rights organizations and scholars are up in arms to protect privacy. Fujitsu's global survey found that 88% of people worry about who has access to their PI, and over 80% expect governments to regulate privacy and impose penalties on companies that don't use PI responsibly [10]. Due to mass media reporting of privacy breaches, executives have had to quit or face lawsuits over data abuses.

As a result, almost every regulatory privacy framework in the world (EU data protection directive 95/46/EC, Convention 108, OECD Data Protection Guidelines, US Bill of Rights Proposal, and more) is now being overhauled with the goal of strengthening consumer rights. However, will regulation and self-regulation initiatives achieve what they say they aim for?

With increasing business interest in personal information and an escalating conflict between privacy rights groups, regulators and industry, we believe that the time is ripe to develop a tenable vision of sharing PI with businesses in PI markets. This vision must allow for an innovative, information-rich world while maintaining privacy. We should embrace the fact that having ubiquitous accessibility to information about us leads to unprecedented insights into our being and new forms of social interaction, eventually improving our quality of life [11]. Fruitful streams of research and innovation depend on data about people. However, harm to human dignity and privacy must be avoided, and people must remain masters of their identities. Neglecting good governance of PI markets could endanger human self-determination and erode the societal advantages of the digital age [12]. What if we had digital markets that used and traded PI whilst allowing people to control their information and identities?

Because of incongruous technical, economic and legal assumptions, it seems that we are far from shaping such a future. Technology scholars have developed privacy-enhancing technologies (PETs) that could put PI management back into consumers' control [13,14]. However, their technical proposals often build on the assumption that people prefer anonymity in transactions with companies [15–17]. Consumers, in contrast, often don't mind being identified in transactions with business partners, and companies are keen to foster 'personal' relationships [18]. While most PET proposals imply that consumers will invest time into privacy management, people simply expect regulators to protect them and companies to behave in an ethical way [10]. Finally, the PET community operates with concepts such as "data minimization" [19], which are hardly

realistic in times when users submit 95 million tweets on Twitter and send about 47 billion (non-spam) e-mails on an average day. The result is a patchwork of PET solutions that are adopted by neither industry nor governments.

Besides the difficulties of deploying easy-to-use PETs, economists disagree about the effects of privacy on welfare [20]. Chicago school proponents argue that PI disclosure benefits society because information asymmetries are reduced [21,22]: as companies learn more about their customers, they can better serve customer preferences. In contrast, critics contend that privacy protection increases social welfare [23]. Everyone acknowledges that people need control over the use of their PI [24,25], but no consensus has been reached on whether people should legally own their PI as a property right [1,25]. Many want to view privacy exclusively as a human rights issue because they are concerned that people could be 'propertized' [3,26], but giving people control over their personal information has driven human rights-based privacy regulation so far [24]. As a result, few scholars have theorized about how PI markets could be organized with privacy in mind [3,9,25,27]. Where scholars have theorized about privacy-enabled PI markets, models have failed to integrate the current technological and legal landscape, and these models provide no pathway to implementation.

This chapter provides the model that we need to make privacy efforts work in current economic environments. Based on insights about consumer behavior, market mechanisms, existing regulation and privacy technologies, we propose a 3-tier model for PI markets. Our model embraces information richness as the future of a digital economy. 'Social data' originating from people will inevitably be an important resource. We acknowledge that many transactions will be identified, however, the market we propose aims to empower people as much as companies. People and companies are assigned a few core rights and obligations, resulting in a new and simple market structure. Many of these rights and obligations are already established, however, they are either weakly enforced or their importance is not recognized by policy makers. In our model, company obligations vis-à-vis consumers are enforced by the law and supported through privacy-enhancing technologies. To make market rules enforceable, our model combines complementary legal and technical enablers. Our model is limited to the private commercial PI sphere, excluding government activity.

In the next section, we describe our model of a functioning PI market in which privacy can be preserved and consumer trust in PI handling can be re-established. In the subsequent sections, this hypothetical market model is described in detail, including the derivation of technical and legal requirements to enforce it. The chapter closes with a critical discussion of our model's benefits and challenges.

1. A Three-Tier Model for PI Markets

The model builds on the existing PI ecosystem. Currently, this system is complex and opaque and its players engage in many secondary data use activities that undermine consumer privacy and trust [4]. We create transparency and simplicity by assigning existing players to a simple three-tier market structure (see Fig. 1). The *first market tier*, which we call "relationship space", includes the business relationship between data subjects and 1st tier partners. For example, a data subject might be a book buyer named Bob, and a 1st tier partner might be an online bookshop called bookshop.com. The *second market tier*, "service space", includes the distributed computing and service infrastructures that enable today's business relationships. It integrates all those proces-

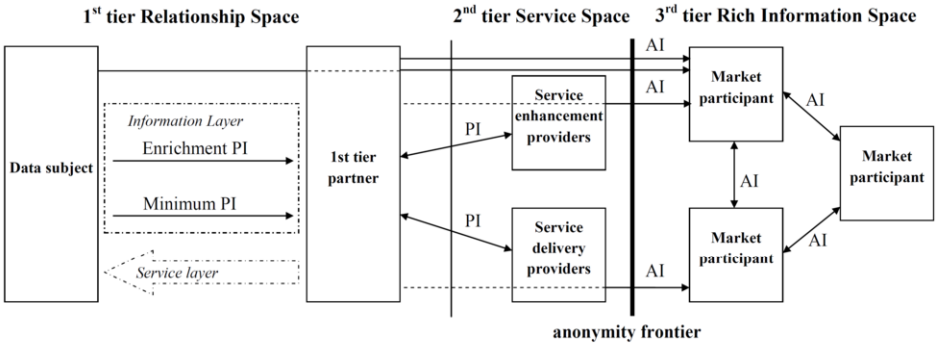

Figure 1. Three-tier model for PI markets.

sors that need to receive customers' PI to directly enable and enrich 1st tier services. We distinguish between service delivery providers, which are necessary to perform the principal service, and service enhancement providers, which contribute to the 1st tier business relationship. For example, bookshop.com's cloud service partner IBX Cloud Services is regarded as a service delivery provider. In contrast, bookshop.com's clickstream research agency Nilsenix is treated as a service enhancement provider. The *third market tier*, "rich information space", encompasses those players who do not directly support the 1st tier relationship. Participants in this part of the market can process as much data as they want, but the data they work on needs to be anonymized – to the degree that it cannot be linked with reasonable effort to 1st or 2nd tier transactions or data subjects. Each time PI is transferred to "rich information space", it has to pass what we call the "anonymity frontier". When information passes the frontier, it loses its personal nature. 3rd tier market participants could, for example, be the traffic monitoring service TraffiMon, which receives anonymized real-time location data from GoogixSmartCars.

The stakeholders in our model are connected by contractual relationships. For any given relationship, market actors (see Table 1) are unambiguously assigned to one of the three tiers. Table 2 summarizes the rights (Right 1–3) and obligations (Obl. 1–9) of all actors in our model. Usually, the data subject and 1st tier partner agree on a contract governing the exchange of service, compensation and PI. Alternatively, their relationship may be governed by legal requirements; for example, mobile operators are legally required to preserve some connection data that they gather about their customers. 1st tier partners arrange service-level agreements with service delivery and enhancement providers specifying the expected service quality. In exchange, service delivery and enhancement providers receive monetary compensation or the right to use and sell anonymized information (AI). Market participants in the 3rd tier close sales contracts over AI with other actors.

1.1. The 1st Market Tier: Relationship Space

The 1st market tier is termed a "relationship space": visible 1st tier partners maintain identified one-to-one relationships with their customers. All PI they receive is the recognized property of their customers and can be used only for purposes set down in PI usage policies, which accompany every PI exchange. The 1st tier has five characteristics: identified business relationships between customers and one visible company, a

Table 1. Actors in the three-tier model and their rights and obligations

Role	Definition
Data subject	Natural person disclosing PI in the course of a service transaction in a business relationship with the 1st tier partner.
1st tier partner	Visible and primary opposite party in the service transaction and, from the viewpoint of the data subject, the party that is responsible for the PI.
Collector	Party that gathers the PI from the data subject either by interrogation or observation.
Controller	"Natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing" of PI (Art 2 Directive 95/46/EC).
Service delivery provider	Entity authorized by the 1st tier partner that is necessary to perform the principal service.
Service enhancement provider	Entity authorized by the 1st tier partner that is not the service delivery provider but contributes by sufficiently close enrichment to the relationship between the 1st tier partner and the data subject.
Market participant	Any party including businesses, private persons, and governments who exchanges AI with other entities in the marketplace.

Table 2. Rights and obligations of actors in the three-tier model

	Property right in PI	Right to a privacy-friendly service	Right to alienate AI	Obtaining legitimization for PI usage	Handling of PI in accordance with PI usage policy	Offering a privacy-friendly service option with minimum PI	Acknowledgement of standardized PI usage policies	Initiating an accountability system	Request for authorization of 1st tier partner when using PI	Separation of PI from multiple data subjects or 1st tier partners	Demonstrate PI usage rights to authorities	Anonymization of information exchanged in the 3rd tier
	1	2	3	1	2	3	4	5	6	7	8	9
Role	Rights			Obligations								
Data subject	x	x										
1st tier partner			x	x	x	x	x	x		x	x	x
Collector			(x)		x					x	x	x
Controller			(x)		x				x	x	x	x
Service delivery provider			(x)		x				x	x	x	x
Service enhancement provider			(x)		x				x	x	x	x
Market participant			x									x

separation of service and information exchange and the right to a privacy-friendly service, legitimized information collection, people's property rights in their personal information, and liability of the 1st tier partner for any PI abuse. The next paragraphs justify these characteristics from an economic and human rights perspective and describe how they can be technically and legally implemented.

Identified Business Relationships and a Unique, Visible 1st Tier Partner. Because personalized customer relationships have proven effective, companies have invested in CRM solutions. Companies need and want identified customer relationships [18]. And many customers are willing to provide their PI in the service context if they receive appropriate returns. Therefore, we depart from traditional data protection models, which promote the idea of total anonymity vis-à-vis companies [15,16].

However, users want predictable relationships in which they can control the use of their PI [28]. Predictability is supported when users deal with only one visible PI-collecting business partner. We define *partner visibility* as a state in which data subjects visiting a physical or electronically enabled premise can unambiguously and effortlessly name the commercial entity that they are transacting with. The brand of this 1st tier partner should be signaled to users when users enter an electronic premise. For example, when a user enters a bookseller portal such as bookshop.com, the visible partner is bookshop.com. Customers in a physical retail store such as Walldepot see Walldepot as the 1st tier partner (and not, for example, the shelf suppliers).

All parties that have a contractual agreement with data subjects must be visible, otherwise the parties are not allowed to collect any PI through mechanisms such as cookies or uploaded software daemons. If data aggregators and brokers want to collect PI from users, they must establish a distinct and visible relationship with data subjects.

The reason for this one-partner rule is that people lose control when multiple parties invisibly collect their PI at the same time. This loss of control promotes distrust on the web [28] and fosters feelings of helplessness in ubiquitous computing environments [29]. From a company perspective, the one-partner rule enables companies to regain the monopoly on PI collection in their transactions. The efforts of companies to build trust in customer relationships are not eroded by a multitude of parallel data collectors. This control increases the power that companies get from competitive information, as unrelated data traders will not have access to identified information.

Selected technical enablers:

- identity and claim assurance
- graphical user interface design.

Legal enablers:

- use of standardized symbols for signaling 1st tier partner
- mandatory principle of "one visible partner"
- legal liability of 1st tier partner for PI use.

Separation of Service and Information Exchange and the Right to a Privacy-Friendly Service. Today, most online transactions are of a composite nature. Information is collected as a service spin-off [30] without making the 'information deal' visible to the customer. In our model, companies are asked to distinguish an information layer and a service layer within a business relationship. The service layer includes the delivery of the principal service to the data subject; for example, the service layer might include the sale and delivery of a book. Within the information layer, PI is split into the information that is needed to deliver a service ("minimum information") and additional information that is used to enrich and enhance the service experience ("enrichment information"). Minimum information can be defined as the set of PI that is necessary and sufficient to perform the principal service. For the online book retailer, the minimum information is the name, delivery address and payment information. The

individual's purchase history, date of birth, and affinity profile, in contrast, is what we consider enrichment information. In our model, these two types of PI are consciously separated. PI used for any purpose beyond the bare minimum of service fulfillment should be presented to individuals as part of a separate transaction. Additionally, partners are obliged to offer one service option (Obl. 3) that requires data subjects to disclose only the minimum amount of their PI. Thus, people always have the right to a privacy-friendly service (Right 2). This right repackages the existing concept of "data minimization" [19] but limits its scope to users preferring data minimization over information rich services.

Consider, for example, a web search engine, look-and-find.com, which offers three service options. Selected by default, the privacy-friendly option requires the individual to pay a subscription fee of € X per month; this option neither records the search queries of the data subject nor shows any personalized ads. In contrast, the second option possibly costs less, for instance € Y per month. This option collects more PI and uses it for an agreed time period to provide a richer service experience, such as individualized search results. The third option commercially leverages users' PI for an agreed time period for purposes such as the targeted placement of ads. This option may be free. The user trades his or her PI in exchange for the free search service. The 'free' mentality governing online business relationships today would make room for a more realistic view of what digital services are actually worth. But PI won't come for free either. Customers would need to knowingly consent to the use of their PI, potentially giving it up in exchange for a free service while being aware that PI is being exchanged for a benefit. The separation of service options benefits all market participants: competition in the market for PI may be improved because the salience of the information transaction increases [30]. In addition to service quality, marketers could compete on PI usage rights and privacy. They could realize new revenue streams from privacy-friendly service options. And people would finally get a true choice of PI disclosure options.

A market challenge is that 1st tier partners could deliberately create opacity by providing a myriad of options, with variations on factors such as retention times or usage purposes for the PI. We therefore see the need for regulators to require standardized PI usage policies, at least for the privacy-friendly baseline offer. To foster enhanced comparability and innovation, minimum information policies shall be standardized (Obl. 4). A further challenge concerns prices for the privacy-friendly default option. Businesses could easily price this alternative highly enough to force people into data disclosure. Regulators would need to prohibit this practice.

Technical enabler:

- standards for the presentation of minimum PI service options.

Legal enablers:

- mandatory separation of the service deal from the PI deal
- obligation to offer one service option with minimum information use at reasonable quality and price (Obl. 3)
- mandatory compliance with standardized privacy policies.

Legitimized Information Collection. The legitimization of data collection is probably the most important bridge between US American and European data protection frameworks [31]. Legitimization justifies the collection and use of PI. It can be obtained either through the informed consent (Obl. 1) of a data subject or by legal empowerment;

for example, mobile operators are legally required to preserve some connection data. Consent is the voluntary, unambiguous, prior, verifiable agreement of the data subject given by an affirmative, not by default action to the 1st tier partner's PI terms [32]. Those terms need to be explicitly communicated to the data subject [33].

Reconsider the search engine example. The default option is the privacy-friendly version of a service. At one click, customers can explicitly opt into the free version. Whatever service option a customer chooses, all parties handling PI must respect the agreement between data subjects and their 1st tier partners as manifested in electronic PI usage policies (Obl. 2).

Software agent solutions, such as P3P agents, enable people to initially configure privacy preferences in their client details once (i.e., in the browser); for example, people might object to data processing for marketing purposes or request immediate deletion of their data. A client-based architecture gives users more control over settings [34]. The user's software agent matches PI usage preferences with companies' standard usage policies (cf. 'Privacy Bird' presented in [13]) and supports the negotiation of an agreed PI usage policy. People are empowered to take advantage of their legal rights in every transaction, and companies benefit from better data quality and compliance.

Technical enablers:

- standards for the presentation and content of PI usage policies
- privacy policy negotiation supported by software agents.

Legal enablers:

- legitimization for PI usage obtained by 1st tier partners
- handling of PI in accordance with electronic PI usage policies (Obl. 2).

Property Rights to Personal Information. A core component of our model is that data subjects have property rights for their PI (Right 1). The property right to PI cannot be alienated [1,25]. Because of its character as a personal right – similar to moral rights in copyright – seizing PI-related rights shall be prohibited. The characteristic of identifiability inseparably binds PI to an individual. Identifiable information can never be an object separable from a beholder in the way that a book can be divided from its owner. However, usage rights to PI can be transferred. From a human rights perspective, data subjects have the biggest interest in the PI asset. Thus, they are the natural holders of this property right.

The main reason for proposing property rights for PI is a psychological one: property rights would create stronger asset awareness in the minds of all stakeholders. The awareness that PI is an asset of economic value makes data subjects more informed when deciding about disclosing PI [35]. Equally, companies will probably be more cautious and reflective in collecting and using it. To make people aware of this asset, we must label information self-determination rights as "property rights".

From a legal perspective, two characteristics set property rights apart from informational self-determination rights in data protection laws: one is the *numerus clausus* and the second is the *erga omnes* effect [24]. A *numerus clausus* of rights is that only one type within the finite set of rights in rem gives the largest extent of control over an object to its holder: the property right. A property right could summarize and simplify the numerous rights of control and access dispersed in data protection laws. The other advantage of property is its *erga omnes* effect: property rights can be enforced against

anyone. Data subjects, consequently, are able to sue any parties infringing on their property right who are not contractual partners or subject to data protection law.

Technical enabler:

- PI usage policy repository on the client side.

Legal enabler:

- recognition of a property right to PI (for an elaborate discussion of the feasibility of this proposal, see [24,25]).

Liability. In our market model, the 1st tier partner is legally liable for any collection and use of PI as well as its contextual integrity. Liability safeguards the data subjects' property right and a contractually agreed-on PI usage policy. PI is abused if it is handled in discordance with the PI usage policy. Liability of the 1st tier partner is natural from a customer perspective. The 1st tier partner acts as the single point of contact for the data subject. For example, data subjects disclosing their PI to bookshop.com feel that bookshop.com is responsible for any abuse – regardless of whether a subcontractor or any other involved party caused the damage. As the 1st tier partner enjoys the benefits of PI use, the partner is also liable for any damage caused through this use. The 1st tier partner, though, can take redress if another accountable 2nd tier party does not adhere to the policy.

Most importantly, we envision that the 1st tier partner is responsible for implementing a technical accountability system that ensures that the PI usage rights that are set down in electronic PI usage policies are obeyed (Obl. 5). Accountability ensures that any access, use, disclosure, alteration, and deletion of PI can be traced by technical means back to the party who has done so. The 1st tier partner shall therefore have a technical infrastructure that can demonstrate PI usage rights to authorities and auditors at any time (Obl. 8).

Technical enabler:

- use of an accountability system to enable and monitor policy-compliant use of PI (e.g. sticky policies, audit logs).

Legal enablers:

- legal obligation to have and regularly audit an accountability system
- liability of 1st tier partner for all PI transactions.

1.2. The 2nd Market Tier: Service Space

Typically, the 1st tier partner is assisted by subcontractors, outsourcers, and strategic alliances to deliver services and products. This complex service web adds to the insecurity of today's personal information markets. In fact, consumers are most concerned about secondary uses of their data by invisible partners [36]. For this reason, we create a "market chunk", organizing this web of invisible service providers. The 2nd tier includes all companies that contribute to the services delivered in the 1st tier. For instance, Datenix provides data that enables bookshop.com to improve users' personalized book recommendations. As a 1st tier partner, bookshop.com is accountable for Datenix's actions. The PI abuse is likely if parties at greater distance from the initial service perceive less responsibility for the PI they use [37].

To extend the context-based trust between data subjects and 1st tier partners, 2nd tier service providers must be legally tied to the initial business relationships. This tie is created via a chain of accountability that ensures authorization, non-repudiation, separation, and auditability. Since all 2nd tier providers need to serve the 1st tier business relationship with the customer, our model ensures contextual integrity of PI use. PI is used within the boundaries of contextual integrity when the applicable social norms of appropriate PI collection and distribution are upheld in a given situation [38]. The following characteristics enable the 2nd tier.

Tying the Service Space to 1st Tier Relationships. We distinguish between service delivery and service enhancement providers (see Table 1). Service delivery providers, such as the parcel services that deliver book orders, are necessary to perform the principal service. They are always immediately involved in the 1st tier relationship; examples of service delivery providers include entities supporting the accountability and security of transactions. Service enhancement providers might also need to receive PI. These providers are parties that *directly* or *immediately contribute* to the 1st tier business relationship. A subcontracting party that receives PI from the 1st tier partner and only uses it for its own interest or the interest of the 1st tier partner is not contributing to the *relationship* between the data subject and 1st tier partner. Directness addresses the factual relation of the enhancement service to the 1st tier partnership, while immediacy refers to the time dimension. Indirect long-term enhancement service providers do not have a sufficiently close correspondence to the business relationship between data subject and 1st tier partner to receive PI. For instance, passing on PI to a market research agency that develops a corporate strategy for the 1st tier partner is out of the context of the initial service transaction. As their consultation threatens to de-contextualize the PI that is employed [19,38], the market research agency is not allowed to use PI in the context of the 1st tier business relationship.

However, business strategy consultants may act as separate 1st tier partners and acquire the right to use PI. In this scenario, two 1st tier relationships would co-exist: one original service delivery relationship and one additional information collection relationship. If a data subject chooses such an enhanced service option, the service delivery providers can also handle enrichment information and service enhancement providers can process minimum information.

Technical enablers:

- privacy policy language
- accountability system to enable and monitor policy-compliant use of PI.

Legal enabler:

- legal obligation to have and regularly audit an accountability system.

Authorization, Non-repudiation, Separation, and Auditability. For 2nd tier parties, an accountability system must comply with the requirements of authorization, non-repudiation, separation, and auditability. First, authorization requires that access to PI by the service provider is approved by the 1st tier partner on an individual transaction basis (Obl. 6). When a customer purchases goods or services, the online shop must explicitly authorize a credit scoring agency to use customer data for a credit check. Second, non-repudiation prevents service providers from falsely denying that they have accessed, used, altered or deleted PI. Third, separation requires that PI units stemming

from different service transactions, data subjects, and 1st tier partners are kept in strict isolation unless the legitimized purpose allows for the combination of PI (Obl. 7). For instance, a billing provider is not allowed to combine the PI from bookshop.com customers and bank customers. This practice safeguards contextual integrity. Fourth, auditability ensures that compliance can be demonstrated at any time to authorities and auditors (Obl. 8).

Technical enabler:

- use of an accountability system to monitor policy-compliant use of PI (e.g. sticky policies, audit logs)
- accountability system to enable and monitor policy-compliant use of PI.

Legal enablers:

- separation of PI from multiple data subjects or 1st tier partners
- legal obligation to and auditing of the accountability system.

1.3. The 3rd Market Tier: Rich Information Space

The 3rd tier is a market space where businesses, individuals, governments, and other parties not contributing to an identified business relationship freely exchange and trade information. They, however, need to ensure *anonymity* according to state-of-the-art technical standards. PI may originate from data subjects, but when the anonymity frontier is passed, this information becomes a *freely exchangeable* good. This asset is usable for innovative services or research. Innovation can be significantly promoted, vividly spurred on the basis of this data. We assume that the marginal utility from identification outside of business relationships is so minimal that it does not justify the ensuing privacy risks. Severe *sanctions* should be imposed on 3rd tier market players who distort competition by holding identifiable or re-identifiable data.

Anonymity. Data subjects want to retain control over the distribution of their PI. They want to share in peace of mind. A straightforward way to create control and peace of mind is to legally enforce anonymity of all data, except in situations where identification is needed or desired by the customer (1st and 2nd tier). People are granted a privacy commons; a shared space of anonymity [25]. In our model, this space is created by ensuring that PI cannot leave the contextual boundaries of the 1st and 2nd tier. When it does, it must be anonymized. What constitutes sufficient anonymization is a dynamic concept dependent on the current state-of-the-art of technology. Regulators should document and update current standards for anonymization in "best available techniques reference documents" (BREFs), which have been applied successfully for integrated pollution prevention and control (IPPC, Directive 2010/75/EU). Currently, the concepts of "k-anonymity" [17], "l-diversity" [39] and "t-closeness" [40] suggest that it is sufficient to have a large anonymity set of individuals, diverse attribute values and similar attribute value distributions. Each market participant in the 3rd tier is obliged to respect these anonymity mechanisms (Oblg. 9) and is regularly audited for the fulfillment of this requirement. Specific PI that cannot be anonymized, such as genetic information, would require separate legislation.

Technical enabler:

- anonymization.

Legal enabler:

- legal obligation and auditing of anonymity requirement in 3rd tier.

Sanctions. In a trustworthy market regime, anonymity is protected by damages and penalties for the illegal acquisition, possession, use or sale of identifiable information. Any entity in the role of a 3rd tier market participant is not allowed to hold PI. If any such entity is caught engaging in PI storage or processing, it shall pay damages to data subjects, partners and others, and pay substantial punitive damages [41]. Moreover, any persons involved in illegal activities shall face criminal prosecution, as they have encroached upon the fundamental rights of other individuals.

Legal enabler:

- sanctions for breaking the anonymity rule.

Free Exchange. Free trade of anonymized information increases the amount of exchanged information. Our market model reduces the amount of legislation or other barriers restricting the alienation of anonymized information. Unhindered trans-border flows of anonymous information are fostered. Any market participant shall have free access to the 3rd tier market, including data subjects who may want to sell their anonymized information directly. As compensation for the costs 1st tier partners incur in our model, they have the right to anonymize and sell any PI collected independently of the data subjects' consent. Market participants can resell anonymized data once they acquire it (Right 3).

Legal enabler:

- right to alienate anonymized information.

2. Implementing the Three-Tier Model

As has been outlined throughout Section 1, technical and legal enablers are required to support the implementation and enforcement of our model. Many of these technologies and legal enablers already exist. This section outlines how our model builds on existing enablers and identifies the enablers that need to be developed or changed.

2.1. Technical Enablers

Well-established privacy-enhancing and security technologies enable the enforcement of our model [42]. Table 3 overviews selected technologies and assigns them to the relevant market tiers. To implement the requirement of accountability in the 1st and 2nd tiers, different systems based on sticky PI usage policies and audit logs are available [14,43,44]. Most accountability systems suitable for ensuring contextual integrity are based on cryptographic technologies that can be easily applied in distributed environments [45,46]. Existing identify technology can determine the party responsible for a data breach. Existing security mechanisms, such as SAML, can identify the 1st tier partner and the data subject [47]. To specify the content of PI usage policies, privacy policy languages are necessary. Some privacy policy languages have already been standardized by the W3C consortium (P3P). Since negotiating these policies is a labo-

Table 3. Existing technologies to support enforcement in the market tiers

Relationship Space (1st tier)	Service Space (2nd tier)	Rich Information Space (3rd tier)
Accountability system Sticky policy, Privacy injector, Privacy-aware access control, Distributed auditing logs		*Anonymization* k-anonymity, l-diversity, t-closeness, Graph anonymity
Identity mechanisms SAML, OAuth, OpenID		
Contextual integrity-compatible cryptography Identifier-based encryption, NOYB		
Privacy policy languages POL, PrimeLife policy language, E-P3P, EPAL, Rei, EnCoRe, PERFORM, Ponder, Contextual integrity language		
Privacy policy negotiation P3P, PISA		*Privacy-preserving data mining* Randomization, Perturbation, Differential privacy, KD cycle-based data mining
Web anonymity and pseudonymity agents LPWA, Crowds, Hordes, Onion Routing, Mixminion		
Do not track		
Human-computer interface Privacy pictograms, User privacy agent interface design, Visual tagging		

rious and complex task for the data subject and 1st tier partner, architectures can make the task easier by employing software agents that semantically understand policy content [48,49]. The usability of privacy functionality and user agents at the interface between humans and machines is more and more improved [13]. Although data subjects are possibly identified on the application layer, they might want to be anonymous to third parties on the communication layer. To ensure their anonymity, data subjects can employ existing web anonymity technologies that protect the interaction between data subject and business partner [15]. Anonymity on the web can be supported by browser functionality building on the "do not track" concept; this functionality indicates to the communication partner that no PI shall be collected. Additionally, anonymization technologies are needed to realize sufficient anonymization of PI in the 3rd tier [17,39,40]. Data mining technologies that preserve privacy can guarantee endured anonymity [50].

2.2. Legal Enablers

Our model needs not only to be technically feasible, but must also be meaningful to public policy. Policy makers need to know which of the rights and obligations we propose already exist in the current legal framework. One important idea is to consider PI as the private property of data subjects [24]. A property right to PI (Right 1) is reflected in the principles of informed consent (Art 7 Directive 95/46/EC, Art 7 General Data Protection Regulation-draft [51], Para. 7 OECD, Art 2 FTC Fair Information Practices (FIP)) and the right to object (Art 14 Directive 95/46/EC, Art 19 [51]). Informed consent gives data subjects the right to determine what happens to their PI. Data subjects can decide on the *usus*, the right to use the information. The right to object to the processing of PI resembles the elements of excludability and *abusus* of a property right. Data subjects can exclude anyone from using their PI, just as the owner of a book can prevent anyone from reading it. Moreover, they can 'destroy' PI by completely revok-

ing all usage rights for anyone and thus have the PI 'forgotten' (cf. Art 17 [51]). Data subjects cannot have *ius abutendi* – the right to alienate the property right itself. The property right is always bound to their identity. However, the usage right can be alienated. Current data protection legislation does not recognize a property right's *usus fructus*: the data subject's right to receive a share of the fruits from the 1st tier partner's usage of PI [52]. The recognition of full property rights to PI is missing in civil law.

So far, a data subject's right to a privacy-friendly service (Right 2) exists only within a very limited scope. For example, Art 8 Directive 2002/58/EC mandates service providers to offer an option blocking the presentation of calling line identification. A German ban on tie-ins of sales and competitions has failed because of concerns about antitrust issues and limits on a data subject's choice (ECJ C-304/08). A data subject's right to object (Art 14 Directive 95/46/EC, Art 19 [51]) prevents usage of the PI but does not grant data subjects a positive right to a PI-minimal service.

All other obligations in our model already exist in legal frameworks. Obtaining legitimization for PI usage (Oblg. 1) is reflected in the principle of informed consent. Three of our model's obligations can be realized by extending the principles of explicit specification of PI usage purposes (Art 6 Directive 95/46/EC, Art 5 [51], Art 5 Convention 108, Para. 9 OECD, Art 1 FIP): policy-compliant PI use (Oblg. 2), standardized PI usage policies (Oblg. 4), and separated PI handling (Oblg. 7). First, the obligation of handling PI in accordance with an agreed PI usage policy is fulfilled when 1st or 2nd tier parties cannot unilaterally extend beyond the purposes that have been agreed upon with data subjects. Second, standardized PI usage policies extend the principle of purpose specification by restricting the contractual freedom of data subject and 1st tier partner to *pre*-specified modes of PI use. Standardized policies do not imply a legal *numerus clausus* of PI usage contract types, but this is most likely a matter of industry-specific self- and co-regulation. Third, separating the PI of multiple data subjects or 1st tier partners to prevent de-contextualization is automatically ensured if PI cannot be used for purposes other than those specified in the policy.

The obligations to initiate an accountability system (Oblg. 5), to request authorization from the 1st tier partner when using PI (Oblg. 6), and to demonstrate legal compliance (Oblg. 8) are part of the principle of accountability (Art 22 [51], Para. 14 OECD). Implementing an accountability system ensures that 1st and 2nd tier parties are technically capable of complying with the accountability principle. Requesting authorization from the 1st tier partner when using PI is necessary to achieve accountability; this requirement is recognized in Art 2 (f) Directive 95/46/EC, where third parties process PI "under the direct authority of the controller or processor". The accountability principle requires PI users to demonstrate legal compliance. We extend applicable law by requiring companies to ensure policy-compliant data processing by using appropriate technical systems.

Finally, the obligation to anonymize any information exchanged in the 3rd tier (Oblg. 9) already exists, to some extent, in the principle of data quality (Art 6 Directive 95/46/EC). PI should "be kept in a form which permits identification of data subjects for no longer than is necessary […]". To this vague formula, our model adds a clear anonymity frontier that unambiguously determines when anonymization takes place. Best available technique reference documents (BREFs), kept current by data protection authorities, prescribe state-of-the-art anonymization technologies. Moreover, our model supports an information-rich space by imposing more stringent sanctions for the abuse of identified information than are currently in place [41]. To conclude, our model's

rights and obligations can be implemented by making only minor adaptations to the current legal framework.

3. Discussion

We are aware that many of the rights, obligations and legal and technical enablers we propose are not new. They have been proposed for over two decades by researchers in privacy, identity, security, and legal studies and debated by companies and regulators. For example, we do not need new security mechanisms to identify the 1st tier partner; we can build on existing technologies, which were outlined in Section 2.1. However, no one has demonstrated how all of the puzzle pieces could be arranged in a market model to benefit both individuals *and* companies.

For personal information markets to benefit both individuals and companies, the enforcement of market rules must be improved. The main design principle of our market model is to combine legal and technical mechanisms, overcoming the weaknesses that each type of mechanism has on its own. A legal property right to PI backed up by technical accountability of data usage simplifies access to law enforcement for data subjects.

One burden that companies will have to carry is to finally provide people with a privacy-friendly default service option. But, as we have shown in this chapter, the burden isn't that heavy. Companies can re-enter competition on the basis of service quality. Furthermore, our model meets the privacy preferences of different individuals: access to content at potentially lower cost for those who are willing to 'pay' with their PI and alternative versions for customers who are concerned about their privacy. Privacy rights proponents may argue that this preference-based market structure disadvantages the poor, who may be forced to sell their PI. This argument is true only if marketers choose to have people pay for the privacy-friendly version. Marketers could also make the data-rich version more attractive from a service perspective – with greater functionality and no ads – while offering a baseline: privacy-friendly service with non-personalized ads.

With respect to the default privacy-friendly version, we suggest regulating the identified market space. One market regulation may be enforcing a price cap and a minimum service quality obligation for privacy-friendly services. Price regulation is common for many service and product areas, including books, public housing, water and electricity, and parks and roads. And even if people were asked to pay more than they do now, we argue that other services areas have seen successful transitions from an initial free offering to paid-for offerings: for example, the short message service (SMS) has become an important source of income for mobile operators even though it was initially a free by-product of telephony services. Finally, even if individuals opted into the usage of their PI in exchange for the service, our market proposal provides privacy protection: companies would be accountable and liable for how they use PI. Limitless reuse and repackaging out of context would be outlawed. Privacy risks would hence be limited, even for those who share. As data subjects will have property rights to their PI, they will also be brought back to the negotiating table. Property rights, a right to privacy-friendly service options and defaults, company accountability and a transparent market structure promise to re-establish the trust we need if we are to see information services flourish.

A core benefit of our model is also its main technical challenge: the creation of a free market space that ensures anonymity. Ensuring anonymity becomes more difficult as technology becomes more powerful, facilitating identification. Anonymization could reduce the entropy of information to such an extent that the utility for information users would vanish. For multidimensional PI that contains many attributes about data subjects, the "curse of dimensionality" forces that information to be extensively aggregated to guarantee reasonable anonymity [50]. Utility-based privacy preservation, however, guarantees that the utility of anonymized data does not drop by more than a defined threshold ε, known as ε-differential privacy [53,54]. Data protection authorities define the "BAT" (Best Available Techniques) (Directive 2010/75/EU) that guarantee sufficient anonymity. Flourishing service spaces based on "non-identified, social data" instead of "personal data" may be the result. Information buyers want to obtain a representative sample of a population of individuals, not the information of identified single data subjects [50].

Some information buyers in the current PI ecosystem cannot use anonymized information and require identities. One example is genetic researchers, who inherently operate on the individual's genome code. Such fields, though, would not be excluded from gaining access to PI. Every party requiring PI can take on the role of a 1st tier partner and purchase the information with the informed consent of the data subject.

Another benefit we see is that our model builds on readily available technologies. Technical feasibility depends heavily on whichever infrastructure changes are necessary to put the proposal into effect. Ideally, the enforcement of property rights to PI would require technology that can trustfully certify the identities of property right holders and data subjects [55]. Unfortunately, waiting for the missing identity layer on the Internet [56] would probably be like waiting for Godot. Consequently, our proposal would be interoperable with, but does not necessarily require, additional large-scale technical infrastructure – such as an identity layer – on the Internet. The technologies compatible with our model, as described in Section 2, can be readily implemented by 1st tier partners.

Finally, two more fundamental challenges of our model must be considered: the concern of 'monopolizing' information and the international enforceability of our model. The idea that personal data could be recognized as property originated in the US; this idea has been met by the criticism that people shouldn't be 'propertized' [3,26] as well as a series of other arguments (for an overview see [25]). Ralph Waldo Emerson once remarked, "As long as our civilization is essentially one of property, of fences, of exclusiveness, it will be mocked by delusions." For these reasons, we view the idea of property rights to PI critically. However, because markets already treat PI as property, we ask only that individuals are accorded the same rights that companies have already claimed for themselves. Moreover, a property right would not substitute but enhance the status of privacy as a basic human right [24]. In Europe, it would provide people with an additional legal instrument, giving them easy access to existing, well-proven enforcement structures. Data subjects would be enabled to effectively claim their rights to PI on their own instead of calling on data protection authorities. Even though data protection authorities have tried to support data subjects in cases of data breach, their effectiveness is limited. Their independence stands on shakier ground than those of ordinary courts. Most importantly, they do not have the capacity to handle the volume of cases that require settlement in personal data markets. It therefore seems more appropriate to give data subjects access to existing law enforcement infrastructure.

Another challenge to our model is its international practicability. Recent years have shown how difficult it is to reach international consensus on data protection or privacy. Enforcement is even more difficult. The Safe Harbor Agreement between the US and Europe on data handling practices is a good example of failure. A more effective path might be to implement and enforce binding, hard law for data protection. For example, property rights are enforceable as well-recognized legal instruments in both the European and US legal orders. If Europe and the US applied property rights to PI [57], the rest of the world would potentially follow suit.

4. Conclusion

For information about individuals to be used effectively, participants in the digital economy must have enough trust to willingly share and exchange information. "Social data" is becoming an increasingly important ingredient for innovative companies; the use of PI is applied with astonishing accuracy by applications that predict traffic jams and monitor public health in real time. Notwithstanding the increasing regulation of data protection and privacy, individuals feel their privacy is being progressively undermined by collecting, aggregating, storing, exchanging, and selling PI for opaque purposes and with shallow consent. Similarly, organizations using PI are worried about unpredictable consumer backlash. The missing governance of personal data markets threatens the autonomy of individuals and undermines the benefits of having an abundant amount of information available. Markets for PI based on property rights have long been recognized as an alternative, but early proposals, not clearly delineating themselves from 'propertizing' data subjects, have been viewed in a suspicious light by data protection proponents.

Our vision for a personal information market could pave the way to a consensus between players in the current PI ecosystem and data protection proponents. Our model embraces data richness as the future of a digital economy, and creates room for information-rich services and data trading as well as identified customer relationships. To help people understand their transactions with companies and the value of their PI, we create a new and simple market structure that assigns clear rights and obligations to all market players. Trust built by a clear allocation of rights also aids companies and legal enforcers. At the same time, our technical and legal suggestions facilitate the ideals of digital enlightenment by empowering people to participate in PI markets and protecting their privacy.

Acknowledgement

We would like to thank Julian Cantella for the editing of the text.

References

[1] Bergelson, V.: It's Personal But Is It Mine? Toward Property Rights in Personal Information. UC Davis Law Review 37, 379–451 (2003).
[2] WEF: Personal Data: The Emergence of a New Asset Class, World Economic Forum, Jan (2011).

[3] Noam, E.M.: Privacy and Self-Regulation: Markets for Electronic Privacy. In: Wellbery, B.S. (ed.) Privacy and Self-Regulation in the Information Age, pp. 21–33. NTIA (1997).
[4] WEF: Rethinking Personal Data: Strengthening Trust, World Economic Forum, May (2012).
[5] Angwin, J.: Online Tracking Ramps Up – Popularity of User-Tailored Advertising Fuels Data Gathering on Browsing Habits. Wall Street Journal, June 18, B1 (2012).
[6] Brock, J.: Introducing Privacyfix: Now it's up to you. Privacychoice, Oct 9, 2012, http://blog.privacychoice.org/2012/10/09/your-privacy-simplified/.
[7] Bott, E.: The Do Not Track Standard has Crossed into Crazy Territory, Oct 9, 2012, http://www.zdnet.com/the-do-not-track-standard-has-crossed-into-crazy-territory-7000005502/.
[8] Tißler, J.: Heftig: iPhone und iPad speichern Location auf Schritt und Tritt. t3n Open Web Business, April 20 (2011).
[9] Laudon, K.C.: Markets and Privacy. Communications of the ACM 39, 92–104 (1996).
[10] Personal Data in the Cloud: A Global Survey of Consumer Attitudes, Fujitsu Res. Inst. (2010).
[11] Cheng, W.C., Golubchik, L., Kay, D.G.: Total Recall: Are Privacy Changes Inevitable? In: Proceedings of the 1st Workshop on Continuous Archival and Retrieval of Personal Experiences, pp. 86–92. ACM, New York, USA (2004).
[12] Metakides, G.: Foreword. In: Bus, J., Crompton, M., Hildebrandt, M., Metakides, G. (eds.) Digital Enlightenment Yearbook 2012, pp. v–vi. IOS (2012).
[13] Cranor, L.F., Guduru, P., Arjula, M.: User Interfaces for Privacy Agents. ACM Transactions on Computer-Human Interaction 13, 135–178 (2006).
[14] Karjoth, G., Schunter, M., Waidner, M.: Privacy-Enabled Services for Enterprises. In: Proceedings of the 13th International Workshop on Database and Expert Systems Applications (DEXA), pp. 483–487, Aix-en-Provence (2002).
[15] Gritzalis, S.: Enhancing Web Privacy and Anonymity in the Digital Era. Information Management & Computer Security 12, 255–287 (2004).
[16] Bella, G., Giustolisi, R., Riccobene, S.: Enforcing Privacy in E-commerce by Balancing Anonymity and Trust. Computers & Security 30, 705–718 (2011).
[17] Sweeney, L.: k-Anonymity: A Model for Protecting Privacy. International Journal of Uncertainty, Fuzziness & Knowledge-Based Systems 10, 557–570 (2002).
[18] Spiekermann, S., Dickinson, I., Günther, O., Reynolds, D.: User Agents in E-commerce Environments: Industry vs. Consumer Perspectives on Data Exchange. In: Eder, J., Missikoff, M. (eds.) LNCS, vol. 2681, pp. 696–710. Springer, Berlin (2003).
[19] Borcea-Pfitzmann, K., Pfitzmann, A., Berg, M.: Privacy 3.0:= Data Minimization + User Control + Contextual Integrity. IT-Information Technology 53, 34–40 (2011).
[20] Acquisti, A.: The Economics of Personal Data and the Economics of Privacy. 30 Years after the OECD Privacy Guidelines. OECD (2010).
[21] Posner, R.A.: The Economics of Privacy. American Economic Review 71, 405–409 (1981).
[22] Calzolari, G., Pavan, A.: On the Optimality of Privacy in Sequential Contracting. Journal of Economic Theory 130, 168–204 (2006).
[23] Acquisti, A., Varian, H.R.: Conditioning Prices on Purchase History. Marketing Science 24, 367–381 (2005).
[24] Purtova, N.: Property Rights in Personal Data: A European Perspective. Dissertation, Uitgeverij BOXPress, Oistervijk (2011).
[25] Schwartz, P.M.: Property, Privacy, and Personal Data. Harvard Law Review 117, 2056 (2003).
[26] Cohen, J.E.: Examined Lives: Informational Privacy and the Subject as Object. Stanford Law Review 52, 1373–1437 (1999).
[27] Aperjis, C., Huberman, B.: A Market for Unbiased Private Data: Paying Individuals According to Their Privacy Attitudes. HP Working Paper, (2012).
[28] Smith, H.J., Milberg, S.J., Burke, S.J.: Information Privacy: Measuring Individuals' Concerns About Organizational Practices. Management Information Systems Quarterly 20, 167–196 (1996).
[29] Spiekermann, S.: Perceived Control: Scales for Privacy in Ubiquitous Computing. In: Acquisti, A., Vimercati, S.D.C.d., Gritzalis, S., Lambrinoudakis, C. (eds.) Digital Privacy: Theory, Technologies and Practices, pp. 5–25. Taylor & Francis, New York (2005).
[30] Jentzsch, N., Preibusch, S., Harasser, A.: Study on Monetising Privacy: An Economic Model for Pricing Personal Information. ENISA (2012).
[31] Oetzel, M.C., Spiekermann, S.: A Systematic Methodology for Privacy Impact Assessments – A Design Science Approach. (forthcoming 2012).
[32] Pachinger, M.M.: Der neue "Cookie-Paragraph" – Erste Gedanken zur Umsetzung des Art 5 Abs 3 E-Privacy-RL in § 96 Abs 3 TKG 2003 idF BGBl I 2011/102. jusIT 2012/8 (2012).
[33] Art29WP: 01197/11/EN WP 187 – Opinion 15/2011 on the Definition of Consent, Article 29 Data Protection Working Party, adopted on 13 July (2011).

[34] Spiekermann, S., Cranor, L.F.: Engineering Privacy. IEEE Transactions on Software Engineering 35, 67–82 (2009).
[35] Spiekermann, S., Korunovska, J., Bauer, C.: Psychology of Ownership and Asset Defense: Why People Value Their Personal Information Beyond Privacy. In: Proceedings of the International Conference on Information Systems (ICIS), Orlando, FL, USA (2012).
[36] Culnan, M.J.: "How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use. Management Information Systems Quarterly 17, 341–363 (1993).
[37] Art29WP: 00264/10/EN WP 169 – Opinion 1/2010 on the Concepts of "Controller" and "Processor", Article 29 Data Protection Working Party, Adopted on 16 February 2010 (2010).
[38] Nissenbaum, H.: Privacy as Contextual Integrity. Washington Law Review 79, 119 (2004).
[39] Machanavajjhala, A., Kifer, D., Gehrke, J., Venkitasubramaniam, M.: l-diversity: Privacy Beyond k-anonymity. ACM Transactions on Knowledge Discovery from Data 1, 3 (2007).
[40] Li, N., Li, T., Venkatasubramanian, S.: t-Closeness: Privacy Beyond k-Anonymity and l-Diversity. In: Proceedings of the 23rd IEEE International Conference on Data Engineering (ICDE), pp. 106–115 (2007).
[41] Traung, P.: The Proposed New EU General Data Protection Regulation – Further Opportunities. Journal of Information Law and Technology 2, 33–49 (2012).
[42] Shen, Y., Pearson, S.: Privacy Enhancing Technologies: A Review. Report HPL-2011-113, Hewlett-Packard Laboratories (2011).
[43] Ringelstein, C., Staab, S.: DIALOG: Distributed Auditing Logs. In: Proceedings of the IEEE International Conference on Web Services (ICWS) pp. 429–436, Los Angeles, CA, USA (2009).
[44] Mont, M.C., Pearson, S., Bramhall, P.: Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services. In: Proceedings of the 14th International Workshop on Database and Expert Systems Applications (DEXA), pp. 377–382, Prague (2003).
[45] Mont, M.C., Bramhall, P.: IBE Applied to Privacy and Identity Management. Technical Report HPL-2003-101. Hewlett-Packard Laboratories (2003).
[46] Guha, S., Tang, K., Francis, P.: NOYB: Privacy in Online Social Networks. In: Proceedings of the 1st Workshop on Online Social Networks, pp. 49–54. ACM, Seattle, WA, USA (2008).
[47] Recordon, D., Reed, D.: OpenID 2.0: a Platform for User-Centric Identity Management. In: 2nd ACM Workshop on Digital Identity Management, pp. 11–16, Alexandria, VA, USA (2006).
[48] P3P: The Platform for Privacy Preferences 1.1 Spec., W3C, 13 Nov (2006).
[49] Borking, J.: Privacy Incorporated Software Agent (PISA): Proposal for Building a Privacy Guardian for the Electronic Age. In: Federrath, H. (ed.) Anonymity 2000, LNCS, vol. 2009, pp. 130–140. Springer, Berlin (2001).
[50] Aggarwal, C.C., Yu, P.S.: A General Survey of Privacy-Preserving Data Mining Models and Algorithms. In: Aggarwal, C.C., Yu, P.S. (eds.) Privacy-Preserving Data Mining, vol. 34, pp. 11–52. Springer, New York (2008).
[51] COM: Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), European Commission, Jan 25 (2012).
[52] Demsetz, H.: Toward a Theory of Property Rights. The American Economic Review 57, 347–359 (1967).
[53] Ghosh, A., Roth, A.: Selling Privacy at Auction. In: Proceedings of the 12th ACM Conference on Electronic Commerce (EC), pp. 199–208. ACM, San Jose, CA (2011).
[54] Dwork, C., McSherry, F., Nissim, K., Smith, A.: Calibrating Noise to Sensitivity in Private Data Analysis Theory of Cryptography. In: Halevi, S., Rabin, T. (eds.) TCC 2006. LNCS, vol. 3876, pp. 265–284. Springer, Berlin (2006).
[55] Sholtz, P.: Economics of Personal Information Exchange. First Monday 5, (2000).
[56] Cameron, K.: Laws of Identity, Microsoft (2005).
[57] Purtova, N.: Property Rights in Personal Data: Learning from the American Discourse. Computer Law & Security Review 25, 507–521 (2009).