Jentzsch, Nicola

Research Report

State-of-the-Art of the Economics of Cyber-Security and Privacy

IPACSO - Innovation Framework for ICT Security Deliverable, No. 4.1

Suggested Citation: Jentzsch, Nicola (2016) : State-of-the-Art of the Economics of Cyber-Security and Privacy, IPACSO - Innovation Framework for ICT Security Deliverable, No. 4.1, Waterford Institute of Technology (WIT), Waterford, http://ipacso.eu/downloads/category/9-ipacso-project-public-deliverables.html?download=27:ipacso-state-of-the-art-economics-of-cyber-security-and-privacy-4-1

This Version is available at:
https://hdl.handle.net/10419/126223

Deliverable D4.1

State-of-the-art of the Economics of Cyber-security and Privacy

Project Acronym: IPACSO

Document Author: Dr. Nicola Jentzsch (DIW Berlin)

Project Full Title: Innovation Framework for Privacy and Cyber-security Market Opportunities

Grant agreement number: 609892

Document Control Sheet

Project Number	**609892**	
Project Acronym	**IPACSO**	
Work-package:	**4**	
Last Version:	**February 2016**	
Issue Dates:		**February 2016**
Version 18		***Original report***

Classification

This report is:

Draft	
Final	X
Confidential	
Restricted	
Public	X

Partners Owning	DIW Berlin	
Author	Dr. Nicola Jentzsch (DIW Berlin, Germany)	Author
Reviewer	Jamie Power (RIKON, Ireland)	Review only (date 20.2.2014)
Reviewer	Zeta Dooly	Review only (November 2014)

The views stated in this report do not reflect the opinion of the DIW Berlin.

Table of Contents

List of Tables

List of Figures

List of Boxes

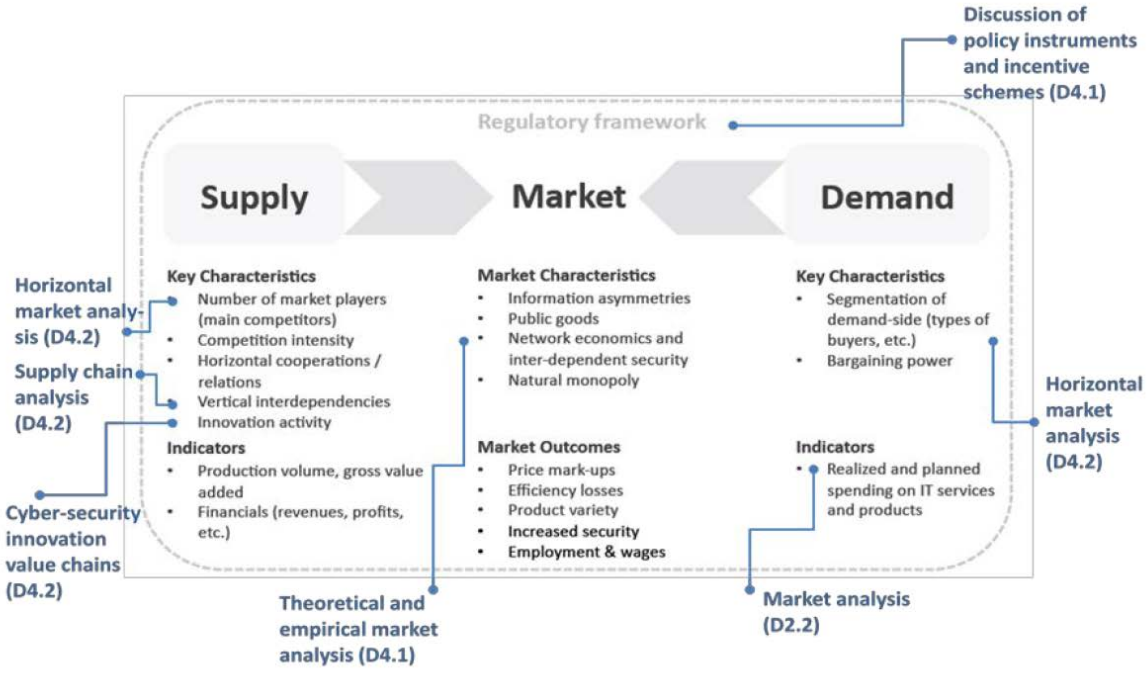
Preface

IPACSO is an EU-funded Co-Ordination and Support Action (CSA) project aimed at supporting Privacy and Cyber-security innovations in Europe. The key aim is to support ICT Security innovators with state of the art innovation methodologies and best practices that improve their overall innovation process. IPACSO will focus on adapting existing innovation methodologies available in other domains, both general and specific, optimizing these approaches for the Privacy and Cyber-Security (PACS) market domains. Ultimately, IPACSO will combine innovation support modules based on establish methods (both generic and technology-specific), with new innovation support approaches geared toward the specific needs of the European PACS marketplace. Market information of high-relevance to PACS innovators will also be included in the project.

From an outreach perspective, innovators working alongside IPACSO will be able to increase their understanding of existing methodologies, best practices, market considerations, economic incentives and share key opinions alongside other peer experts in the PACS domain. By reaching out to IPACSO, privacy and cyber-security innovators will be put in touch with other innovators, business support organizations and financing. With IPACSO, privacy and cyber-security innovators will be getting additional promotion for their innovations, as IPACSO specifically focuses on innovations.

The following scheme outlines in brief the relation of the two deliverables D4.1 and D4.2 to the developed Privacy and Cyber-Security Market Scheme. It enables the reader to see what is covered in the different deliverables and to what deliverable he/she needs to turn in order to find the information of interest.

Cyber-Security Market Scheme and IPACSO Deliverable



Executive Summary

This document is an overview of the state-of-the-art in the economics of Privacy and Cyber-security (PACS). It is the Deliverable D4.1 under the FP7-financed project "Innovation Framework for Privacy and Cyber-security Market Opportunities." This is the most comprehensive overview on the economics of PACS to date.

This document is intended for a diverse readership. Policymakers may use it in order to obtain an overview of the most recent research and insights that can be derived on the effectiveness of specific policy measures (such as data breach notifications). Researchers can use it as introductory reading and to obtain an overview of the field. Innovators and entrepreneurs may use this report to obtain a better understanding of the market they are operating in.

It is stated that Privacy and Cyber-security markets differ from bricks-and-mortar markets because of the immateriality of the products and services provided and because of amplified network externalities that exist in these markets. These can lead to inefficiencies in terms of social welfare, misleading price signals or even market breakdown.

The first chapter of this report introduces the reader to the basic concepts of economics, economic incentives and incentivization as well as to decision-making in the cyber-security domain. It covers proactive and reactive investment strategies, components of the cost/benefits of PACS investments and the security returns on investment model.

The diverse field of cyber-economics is then mapped by sorting the research works into 5 areas: (1) game-theoretical approaches to cyber-security; (2) Experimental and psychological research; (3) Victim studies; (4) Methodological Advances; and (5) Other research. One of the most important parts of the document is the discussion of market failures in cyber-security markets and problems such as information asymmetries, networks externalities, public goods, interdependent security and natural monopoly cost structures.

In the chapter on the economics of privacy, basic concepts are discussed such as the different types of transactions that exist. The literatures in this field are sorted into the following categories: (1) Empirical works (laboratory experiments and surveys); (2) Hypothetical scenarios; (3) Field experiments (including survey-based experiments); and other research (including methodological advances). Market failure problems are also discussed for markets for personal data products/services and privacy products/services.

Other topics covered in that chapter span from the challenges of privacy preference measurement to the development of privacy metrics. Moreover, attention is also devoted to the monetization of privacy and the economic value of personal data with different methods to obtain estimates of valuations. The conclusion from these sections is that it is a great challenge if not impossible to obtain an unbiased and exact estimate of the valuation of personal data. Much more effort needs to be invested in developing robust market mechanisms, where data subjects can actively participate.

The report further covers policy-instruments and incentive schemes in the area of PACS, ranging from mandatory to voluntary instruments. Finally, the report concludes with an overview of research challenges for further work and for the future H2020 agenda.

I. BASIC CONCEPTS AND TERMINOLOGY

1.1 THE CYBER-SECURITY MARKET

Cyber-security (or ICT security) is of utmost importance as an input into the critical infrastructures in Europe. Its importance will increase in future with technological developments such as cloud computing, the Internet of Things, mobile deployments, and Big Data applications. However, currently we lack a standardized and acknowledged method for identifying the size of cyber-security markets in Europe, the main players, their competitiveness and innovation potentials. This situation impairs any evidence-based targeted economic or industrial policy. The purpose of this section is to give a short overview of the industry and market.

Although we lack a common definitional and classificatory base, consultancy firms have published a number of proprietary reports on cyber-security markets in Europe. For example, ADSResearch estimates that the global cyber-security market in 2014 reaches 76.68 billion USD.[1] There are a small number of public reports covering selected countries, including Germany (Bundesministerium für Wirtschaft und Technologie 2013), the United Kingdom (Pierre Audoin Consultants 2013) and Spain (Inteco 2009). These provide some insights on potential industry and market classifications. Note that here, industry and market are not used interchangeably: industry consists of suppliers, the market consists of a physical and/or virtual place, where the supply and demand for PACS products and services meet.

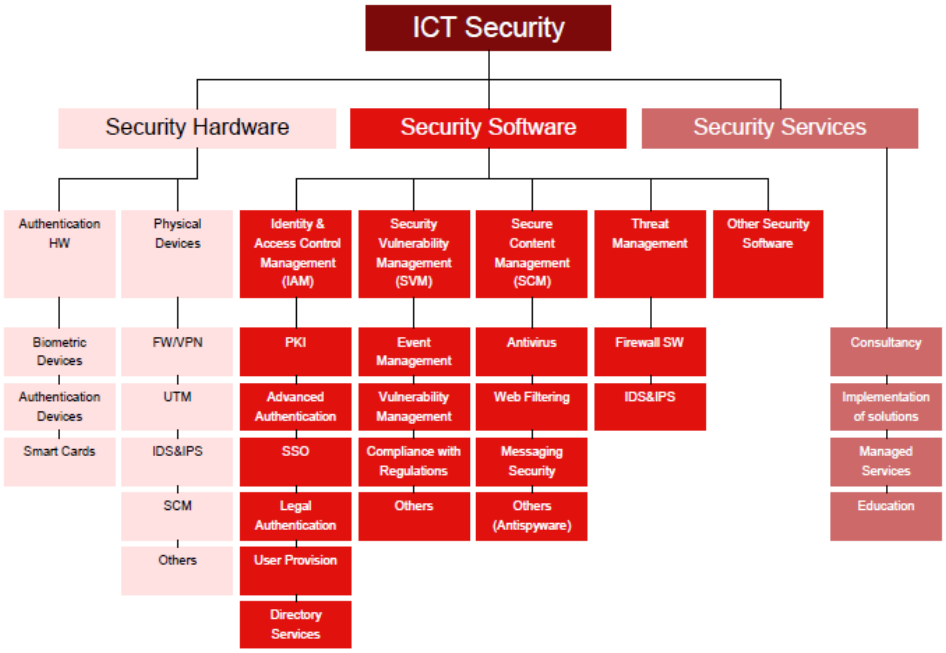
IT security products and services are a downstream market of the IT industry, because they enable the functioning, integrity and reliability of computing resources and IT systems. One **industry classification** used by different institutions is the functional segmentation into software, hardware and services (see Bundesministerium für Wirtschaft und Technologie 2013, IDC EMEA 2009). This classification allows alignment with international classification systems (such as the NACE system), although these frequently do not provide the detail needed to identify exactly the cyber-security industry. As the main focus here is to give a brief overview, it is not elaborated on methodological details. For these, the interested reader is referred to the referenced reports.

One approach segments the market into four buyer sub-segments: (1) defence and intelligence, (2) government (other than defence and intelligence), (3) enterprises, as well as (4) SME & consumers. Another approach segments the market according to the security solution sought (e.g. network security, hardware security, app security and data security, among others (Bernnat et al. 2010: 25). The business models, go-to-market strategies and innovation cycles in these sub-segments vary strongly. It depends on the entity's goals, what segmentation methodology should be used.

Figure 1 combined the first segmentation with that last one mentioned, i.e., the security solutions. More detailed market analyses are presented in the IPACSO project in D2.2 and D4.2.

[1] See company website: https://www.asdreports.com/shopexd.asp?id=98074

Figure 1 Classification of ICT Security Market



Source: IDC quoted in INTECO (2009)

One of the most critical questions is whether the cyber-security and privacy market differs from any other market. We think that this is the case. The first reason is the immateriality and complexity of the products and services provided and the immateriality of the assets they are supposed to protect. The second is the inter-dependence of security among the different market players, where security or privacy of one player depends on the actions of the others. These are amplified network externalities, a peculiarity of cyber-security and privacy markets.

It is important to note that markets are not a well-suited mechanism to achieve social optimal levels of the provision of a good in the presence of externalities, as will be discussed in the sections on different kinds of market failures.

1.2 An Introduction to Cyber-security and Privacy Economics

Economics enables the strategic analysis of security and privacy problems. Principles of economics can be applied to a problem if there are actors with defined economic or social preferences employing strategies to achieve a certain goal. These actors are rational and if they diverge from the rationality principle they are at least "predictably irrational" (Ariely 2008). Given that actors are rational, they maximize their payoff by minimizing the effort invested to achieve a goal. They normally act under conditions of scarce resources. Moreover, economists study cyber-security and privacy problems in the framework of demand/supply models (i.e. for example the cyber-security market), where IT security and privacy are modelled as rational decisions made by the players involved.

One of the first observations made at the outset of the discussion of cyber-security economics is that security is as much an economic as a technological problem (Anderson and Moore 2006).

Therefore, a better incentive structure might motivate greater investments in cyber-security and privacy. This approach is increasingly stressed in both the U.S. and across Europe. Within the IPACSO framework, the intention is to better understand the incentives of market players to adopt either:

(a) Cyber-security and privacy technologies; or

(b) Frameworks to improve adoption of cyber-security and privacy technologies,

where the main focus is on the former as this will also spark greater innovation. After the section on the basics of cyber-security and privacy, it is discussed **how to incentivize greater security and privacy, where market incentives seem to be insufficient** due to reasons discussed in the upcoming sections. We separate cyber-security economics from the economics of privacy for exposition purposes, although there are some interrelated aspects. Whereas the term cyber-security describes the capacity to detect threats to information systems and to implement measures to reduce them, personal privacy describes situations of asymmetrically distributed private information that is connected to an individual (see section on the Economics of Privacy in this report).

1.2.1 CYBER-SECURITY ECONOMICS

The economics of cyber-security applies principles of economics to the analysis of cyber-security problems, including the lack of adoption of PACS. Basically most analyses are devoted to cost-benefit trade-offs faced by rational market participants, their strategic behaviour and market outcomes in terms of welfare for participants. Cyber-security analyses not only include firms and consumers, but also government and third-party players, including adversaries (hackers, etc.). Moreover, the field also covers the analysis of market mechanisms and market failures as well as the economic impact of regulation on cyber-security. At the core of the economics of cyber-security are security risks. Especially important are financial gains as motivation for cybercrime (ENISA 2012a). A large share of the literature is devoted to modelling cybercrime and cyber-security investment decisions, measurement of cybercrime costs, modelling cybercrime insurance or the welfare effects of information sharing among firms. All of these will be discussed in greater detail below.

1.2.2 ECONOMICS OF PERSONAL PRIVACY

This research area focuses on the application of economic analysis to privacy, where two aspects must be emphasized. First, ***privacy is generic*** if it denotes a general form of information imbalance not connected to a particular person, but to the publicity of the data, i.e. one market participant holds information in private that the other does not have.[2] ***Privacy is personal*** if it is related to an *identifiable individual* that can be singled out from an anonymous mass. Thus, for personal privacy it is important that individuals hold private information that is connected to their identity.[3] And conversely anonymity can be seen as the state of not being identifiable within a set of subjects, the so-called anonymity set (Pfitzmann and Köhntopp 2000). Different degrees of identification can be mathematically defined: the degree of identification increases (and the degree of anonymity decreases) with the probability of being drawn from an anonymous set of individuals. The degree of

[2] For the purchase of an apple at a market it is not necessary to know the name of the buyer. However, the apple seller would like to know the buyer's maximum valuation of the apple, which is the buyer's private information.

[3] See also Jentzsch et al. (2012).

identification (or anonymity) provided by a system does not depend on the size of the anonymity set, but on the distribution of probabilities (Diaz et al. 2002). The academic literature on privacy is divided into works that use the generic approach and works that use the personal one. There are other definitions of privacy, in the legal, technical and philosophical domain, but these are not the subject of discussion or evaluation here, as the focus is on economics and incentives for more privacy.

The economics of privacy focuses on incentives and actions of firms and consumers with respect to personal data. At the core of the analysis are privacy risks (or ambiguity)[4] and the ambivalent welfare effects arising from the disclosure of personal data. Privacy economics focuses on the cost-benefit trade-offs of actors, their strategic actions, market outcomes and market failures, similar to cyber-security economics. Moreover, it also includes the change of the competition among firms that personalize products or services and/or prices, while facing consumers that are heterogeneous in privacy preferences. The economic impact of government regulation is analysed as well.

Frequently recurring topics in the field are the measurement of privacy preferences, interaction of stated preferences (attitudes vs. statements) and revealed preferences, privacy nudges, or the effects of online privacy seals on disclosure behaviour. All of these aspects will be discussed in upcoming sections.

1.3 Generic Introduction to Economic Incentives

The adoption of economic incentives for improved cybersecurity and privacy sets the stage for the study of these problems in a supply/demand framework. This approach has strengths and weaknesses. One advantage is the better understanding of market-driven behaviour and its interrelation with cyber-security and privacy. Moreover, if market failures could be ameliorated, market participants could trend towards the optimal level of investment in IT security. However, there are also drawbacks. The main thrust of the economic literature is devoted to rational choice of agents. But important actors in the cyber-security domain (hackers or disgruntled employees) might not adhere to the traditional cost-benefit calculation. Edward Snowden is an outstanding example of this, among numerous hackers that gain reputation effects from tackling the most secure systems. In these areas, an economic analysis might have weaknesses.

Economic Incentives – An economic incentive is an inducement (motivation) that leads to an action or behaviour, which is rendering a (positive) payoff for the actor. Payoffs are outcomes of cost-benefit trade-offs. A rational actor seeks the optimal choice by maximizing payoff. In economics, utility functions model cost-benefit trade-offs and therefore represent preferences of actors. Where the outcomes of choices are uncertain, risk or ambiguity are introduced into the decision model.

The actor's preferences order the outcomes of different choices he or she is confronted with. If a payoff is positive, it is a reward that provides an incentive for a specific action or behaviour. If a payoff is negative, it is a penalty that acts as disincentive. If incentive schemes are not well designed, they lead to suboptimal choices.

[4] In the economics terminology, the term "risk" describes situations of uncertainty with **known probabilities**, while the term "ambiguity" describes situations of uncertainty with **unknown probabilities**. In decision theory, there is a known cognitive bias in individual decision-makers showing that persons prefer a situation with known probabilities (i.e. risk) over one with unknown probabilities (i.e. ambiguity).

Trade-offs may be solely monetary, but can also involve other – psychological – costs and benefits. For example, if a computer system is compromised and the stolen data are used to commit a financial crime, the damaged party suffers a monetary loss. However, if the security incident is made public, the targeted firm also suffers a reputational damage. Such reputational effects may severely impair (or not) trust that customers place in the firm's security procedures. Psychological effects may also arise on the part of the damaged individual and involve humiliation or anxieties.[5]

As stressed by Gordon (2007: 4) the main objective of cyber-security investments **is to reduce the risk of security breaches**. However, a twin-goal might be the **reduction in variability of potential losses from cybercrime**. The latter increases planning and budgetary stability for companies.

Concept of Incentive-Compatibility – In Game Theory an incentive-compatible mechanism ensures that it is the optimal strategy for economic agents to reveal private information truthfully in equilibrium. For example, a mechanism is incentive-compatible if it provides buyers with the motivation to truthfully reveal their valuation of a good. Strong incentive-compatibility holds that truth-telling is an optimal strategy, independent of the other agents' actions. In this case the mechanism is said to be robust. The weaker technical concept holds that truth-telling is Bayes-Nash equilibrium, i.e. truth-telling is only optimal, if all others do the same.

In the context of this report, we do not use a technical definition, but a more general one that holds that an action is incentive-compatible, if it is in the interest of a participant to adopt that action such as investing in PACS technologies.

1.4 Decision-Making in Cyber-Security

Traditional management models rely on cost-benefit trade-offs in order to assess whether a measure should be implemented or not, i.e. whether investment in PACS is worthwhile. More generally, whether a security strategy is effective or not depends on whether cost-benefit trade-offs can be related to the achievement of the intended goal.

Ideally, a firm facing the decision of the adoption of a new IT security system knows all costs and benefits involved in order to make the optimal decision. However, as firms act under limited information and under budget constraints, the option of spending more funds for improving IT security competes with other options that might improve revenues (such as spending more on marketing).[6] To make matters worse, there are **direct and indirect costs of PACS expenditures**. The direct costs and benefits accrue only to the firm making the decision to purchase PACS technologies. However, indirect costs and benefits may accrue to other market parties. In the value chain, the investment of one firm into a more secure system, indirectly improves other connected firms' security. This is explained in greater detail in the section on network externalities.

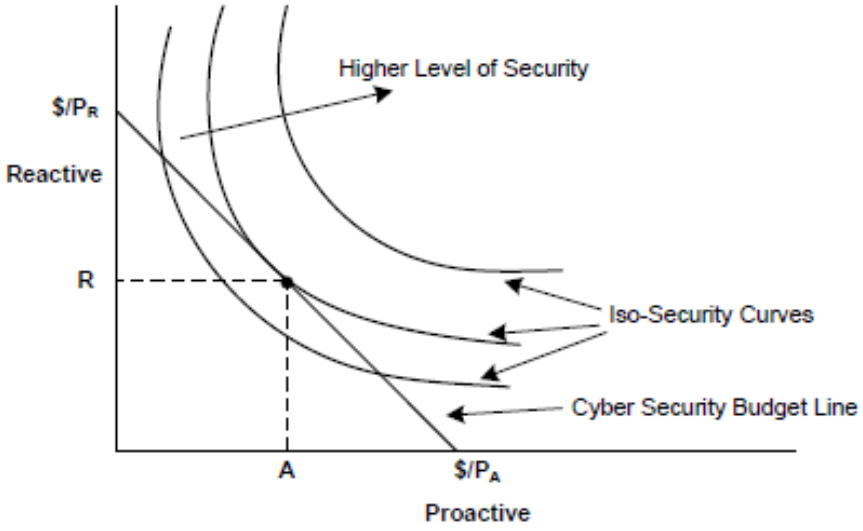
[5] These might arise if personal data (such as name, address, credit card number, etc.) are peddled on a data black market and a number of unidentified criminals have access to the information.

[6] It has been stressed in the literature that IT security investments have primarily a cost-saving character compared to other measures that improve revenues (Gordon 2007; ENISA 2012b)

1.4.1 PROACTIVE AND REACTIVE INVESTMENT STRATEGIES

As surveyed by the Research Triangle Institute (2006), firms face the choice of reactive versus proactive PACS investment strategies. Based upon interviews and case studies of firms in various industries in the U.S., the researchers state that "it is most efficient to rely on existing, proven security technologies and then to be able to quickly implement patches when new viruses are identified." (Research Triangle Institute 2006: 32). This is an observation that seems to be supported by widespread anecdotal evidence, where firms beef up security only after they have been hit by a data breach.[7] Many firms characterized themselves as employing a mix of proactive and reactive security strategies, presented as iso-security curves (**Figure 2**). The further these are away from the origin, the higher the level of security reached.

Figure 2 Firm Selection of Optimal Proactive/Reactive Mix



Source: Research Triangle Institute (2006)

An iso-security curve marks the trade-off of one strategy for the benefit of the other. The optimal mix of proactive and reactive strategies is given at the point of tangency of the budget line with the highest iso-security curve attainable given the budget constraint.

1.4.2 COMPONENTS OF COSTS AND BENEFITS OF PACS PRODUCTS AND SERVICES ADOPTION

Table 1 shows some of the major components of the cost and benefits categories regarding PACS investments. **The difficulty of estimating tangible benefits leads to a problem of making a business case for spending on PACs.** Companies developing innovative PACS products and services will have a problem in making a value proposition, if tangible benefits cannot be ascertained. As discussed above, this can lead to a general deferral of investments by firms into the future. Often, companies only react with increased spending on IT security after a large-scale data breach has occurred and there are indications that this is the most cost-effective way (thus, rational) to do so. However, in case of a data scandal it is relatively easy for IT staff to make a business case for greater IT

[7] See for example, the report CBC News (2014). Target CIO resigns as security revamped over data breach, http://www.cbc.ca/news/business/target-cio-resigns-as-security-revamped-over-data-breach-1.2561648

investment spending. So timing is important for showing the value proposition of innovative PACS products and services, where the best time might be after a firm has been hit by a cyber-attack.

Table 1 Potential Costs versus Benefits of PACS Investments

Costs	Benefits
Personnel costs (set up of new in-house teams, tiger teams, etc.)	Decrease in security incidents & cybercrime losses
Purchase cost (hardware, software, consultancy services)	Reduction in costs of liability for breaches
Administrative costs	Increase in trust of customers
In-house R&D	Increase in company reputation
Opportunity costs*	Protection from unfair competition (industrial espionage)
	Reduction in switching of disgruntled customers to competitors
	Increase in compliance (if a security duty of care is mandatory)

Notes: *Funds spent on IT security cannot be spent for other purposes. Source: The author.

1.4.3 Costs and Benefits of Adopting Innovative PACs

When calculating the cost/benefits associated with the adoption of **innovative** PACS products and services (in this context understood as technologies or procedures not currently in use at the firm in question), the case becomes even more complicated, because more unknown variables enter the calculation. The analysis involves the comparison of new PACS with those currently in use at the firm, which can be updated. While some of the benefits might have been demonstrated by the technology in use, this is not the case for the new technology. This makes it difficult for new technologies to penetrate a market, where existing security systems can simply be updated.

As known from economic research, there is an ambiguity bias in decision makers. This bias describes a preference for technologies in use, which are associated with known risks. For example, the firm has already experience with security breaches and knows at least some of the weaknesses of the system in use. Such is not known for wholly new PACs products and services. These risk perceptions and learning effects (with respect to the system in use) can become a “market barrier.” New PACS need to prove their value added and top current systems in use in order to replace them. Once again, it is difficult to estimate how the probability of a security breach is lowered once new innovative PACS products and services are adopted. This is a threshold to overcome for all firms innovating in the PACS technology space.

1.4.4 Security Returns on Investment Model

There are several models for the calculation of the returns on investment (see Sonnenreich et al. 2006, ENISA 2012b), which are also called security metrics or cyber threat metrics. However, in

general, there is an absence of actuarial tables, from which information on damages based upon real cases can be derived. These tables are typically based upon empirical distributions.[8] The lack of, or weakness in the methods referred to here, makes it difficult to justify PACS investments in firms, as they are often not seen as enabler by the top management of a firm, but as costs.

Returns on Investment $$ROI = \frac{eR - I}{I}$$

ROI is the expected return (eR) minus the investment costs (I) divided by I. For security investments Sonnenreich et al. (2006) propose the ROSI model.

Returns on Security Investment $$ROSI = \frac{(RE)(RM) - I}{I}$$

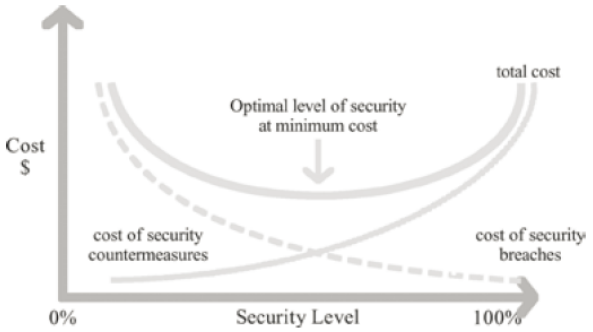
This metric is the risk exposure (RE) times the risk mitigated (RM) minus the I divided by I. RE must be based on past observations, for example the number of attacks by hackers and the damage caused in terms of money. RM is the reduction in risk (for example, the percentage of hacker attacks identified and mitigated). The problem, however, is not to find and develop risk metrics, but to find ***accurate numbers to fill the variables with meaningful values***. Especially tricky is the problem of risk exposure. While (discovered) virus infections or hacker attacks might be countable and their damage assessable, it is questionable whether firms can correctly assess security risks posed by disgruntled workers or by social engineering. Another factor complicating the matter is the ever-changing nature of technology platforms as well the changing nature of datasets and networks (see section on network externalities and interdependent security).

The traditional **Security Returns on Investment model**[9] (see **Figure 3**) sets the costs of security measures in relation to the security level reachable by expending funds. Such models are typically used by the industry to demonstrate the value-proposition of their product. Moreover, decision makers need to employ them in order to compare different investment strategies with relation to PACs. Schneier (2008) critically remarks that increased IT security is an expense for loss prevention and thus it is less about earnings. Moreover, security investments are often considered sunk costs that are not reversible. However, PACS is also increasingly seen as economic enabler (Bundesministerium für Wirtschaft und Technologie 2013). Earnings might increase due to better security, if more consumers switch to the more secure provider. In this case, greater security would reflect in greater earnings. However, it is an open question whether data breaches, for example, lead to a migration/switching to competitors by disgruntled customers (i.e., whether this is a well-designed incentive scheme).

[8] The best data available in the U.S. is from the Computer Security Institute and the U.S. Federal Bureau of Investigation, according to Sonnenreich et al. (2006). In future, gauging the risk will be easier through Big Data analysis.

[9] The Return on Investment is simply the expected from investment minus its costs divided by the costs.

Figure 3 Security Return on Investment Model



Source: Schneier 2001

According to the above model the optimal level of security is reached when the cost of security measures equals the costs of security breaches. Beyond this point, any increase in security expenditures does not compensate for the reduction in the cost of security breaches.

However, the main problem associated with the above is that we have not developed a good understanding of the shape of the cost function based on proper econometric modelling. For example, the cost function could be skewed or discontinuous. More research needs to be invested in the application of empirical techniques to estimate these functions for individual companies and industries. Moreover, the benefits of investing in PACS could be greater than what is captured in the model above, considered the positive externalities that come with it. These are even amplified, if the impact of security incidents on the critical infrastructure is considered, upon whose functioning our society rests.

The calculation of risk arising through mutual exposure, along with other horizontal and vertical relations among market players, is a complex, if not almost impossible task, because it entails access to security information of the interconnected firms. These, however, have in general no incentive to share such information for fear of competition, litigation and reputation effects. The aforementioned network externalities also inhibit accurate calculation of security returns on investment. Sonnenreich et al. (2006) propose a computation of exposure as follows

Annualized loss exposure $$ALE = (SLE)(ARO)$$

which is the product of Single Loss Exposure (SLE) times the Annual Rate of Occurrence (ARO). Again, the problem of correct measurement exists. Future development of metrics ought to account in one way or the other for the aforementioned externalities. Moreover, more effort needs to be put into the potential use of Big Data analysis techniques for gauging cyber-security threats.

Cyber-security Metrics

In the area of **measurement** comprehensive overviews already exist. For example, Herrmann (2007) lists more than 900 security metrics. In Brotby and Hinson (2013) more than 150 metrics are listed, ranging from risk management metrics to IT security metrics to compliance and assurance metrics. The authors have made the list accessible over the Internet by putting it on their website as Excel file.[10] Overviews are also presented by Mateski at al. (2012) and Swanson et al. (2003), among many others. Cyber-resilience metrics are discussed in Linkov et al. (2013). Privacy metrics, an area not well researched, will be discussed in the section of privacy economics.

Box 1 Challenges in Estimation of Risk Metrics

There are great challenges encountered in the calculation of proper values of risk metric variables. Moreover, there is no unified framework how risk metrics ought to be applied.

At the moment, companies use different techniques to evaluate internal costs arising from security incidents. Another challenge is that many security incidences remain undiscovered.

Advice for an Applied H2020 Research Agenda with Respect to PACS

Much more research effort needs to be directed toward the improvement of tools that incentivize PACS technology adoption. Policymakers can play an activating role in this respect. The following is a preliminary list of proposals on what to focus:

- Provision of guidance on security metrics to the industry, including the choice of the right metrics as well as the right estimation techniques, i.e., how the variables can be measured in an economically meaningful way;
- Provision of models and case examples of cost-benefits analyses of IT security investments for firms planning to invest in PACS technologies;
- Provision of more standardized tools to assess risk inherent in IT systems;
- Provision of advice with respect to customer action (switching) after security breaches, that is based upon experimental causality analyses;
- Development of a tool box of how firms can systematically present the value proposition of the PACS products and services they developed to potential end-users; and
- Sourcing of more knowledge (in terms of research) on interconnected risks and mutual exposures as well as spill-over effects of security incidents.

[10] It is downloadable at: http://www.securitymetametrics.com/html/toolkit.html

References to Chapter I

Acquisti, A., Friedman, A. and Telang, R. (2006). Is There a Cost to Privacy Breaches? An Event Study, in (Eds.) Proceedings of the Twenty-Seventh International Conference on Information Systems, 1563-1580. Milwaukee

Ariely, D. (2008). Predictably Irrational: The Hidden Forces that Shape our Decisions (Harper Perennial).

Anderson, R. and T. Moore (2006). The Economics of Information Security, Science (27 October 2006) 314: 610-613

Bernnat, R., Bauer, M., Zink, W., Bieber, N. Jost, D.(2010): Die IT-Sicherheitsbranche in Deutschland. Aktuelle Lage und ordnungspolitische Handlungsempfehlungen. Studie im Auftrag des Bundesministeriums für Wirtschaft und Technologie, Berlin.

Brotby, W.K. and G. Hinson (2013). Pragmatic Security Metrics: Applying Metametrics to Information Security, CRC Press.

Bundesministerium für Wirtschaft und Technologie (2013). Der IT-Sicherheitsmarkt in Deutschland, Grundstein für eine makroökonomische Erfassung der Branche, http://www.bmwi.de/DE/Themen/Digitale-Welt/sicherheit,did=360708.html

Cavusoglu, H., Mishra, B. and Raghunathan, S. (2004). The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. International Journal of Electronic Commerce, 9(1).

Campbell, K., L. Gordon, M. Loeb and L. Zhou (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. Journal of Computer Security, 11(3):431–448, 2003.

Diaz, C., S. Stefaan, J. Claessens and B. Preneel (2002). Towards measuring anonymity, PET'02, Presentation presented by B. Choi, cs6461, Computer Science, Michigan Tech, www.csl.mtu.edu/cs6461/www/Slide/Measuring%20Anonymity02.pdf

ENISA (2012a) Cooperation between CERTs and Law Enforcement Agencies in the fight against cybercrime - A first collection of practices, https://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/supporting-fight-against-cybercrime

ENISA (2012b). Return on Security Investment, http://www.enisa.europa.eu/activities/cert/other-work/introduction-to-return-on-security-investment

Gal-Or, E. and A. Ghose (2005). The Economic Incentives for Sharing Security Information, Information Systems Research 16(2), pp. 186–208.

Gordon, L.A. (2007). Incentives for Improving Cyber-security in the Private Sector: A Cost-Benefit Analysis, http://hsc-democrats.house.gov/SiteDocuments/20071031155020-22632.pdf

Herrmann, D. (2007). Complete Guide to Security and Privacy Metrics Measuring regulatory compliance, operational resilience, and ROI, Auerbach Publications

IDC EMEA (2009). The European Network and Information Security Market – Scenario, Trends and Challenges, April, http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=2153.

INTECO (2009). Study on the ICT security sector in Spain – 1st Report from the Information Security and e-Trust Analysis and Study Group, https://www.inteco.es/CERT/publications/Studies/Study_ICT_security_sector_Spain

Linkov, I., D.A. Eisenberg, K. Plourde, T.P. Seager, J. Allen, A. Kott (2013). Resilience metrics for cyber-systems. *Environment Systems and Decisions*, 33: 4, 471-476

Mateski, M. C.M. Trevino, C.K. Veitch, J. Michalski, J.M. Harris, S. Maruoka, J. Frye (2012) Cyber Threat Metrics, Sandia Report, SAND2012-2427, https://www.fas.org/irp/eprint/metrics.pdf

Muntermann, J. and H. Roßnagel (2009). On the Effectiveness of Privacy Breach Disclosure Legislation in Europe: Empirical Evidence from the US Stock Market, in: Lecture Notes in Computer Science , A. Jøsang, T. Maseng and S. Knapskog (eds.), Springer Berlin / Heidelberg, 1-14.

Pfitzmann, A. and M. Köhntopp (2000). Anonymity, Unobservability, and Pseudonymity – A Proposal for Terminology, TU Dresden.

Pierre Audoin Consultants (2013). Competitive analysis of the UK cyber-security sector, Study, https://www.pac-online.com/competitive-analysis-uk-cyber-security-sector

Research Triangle Institute (2006). Economic Analysis of Cyber-security, AFRL-IF-RS-TR-2006-227, Final Technical Report (July 2006).

Schneier, B. (2008). Security ROI: Fact or Fiction? Data Protection, http://www.csoonline.com/article/446866/security-roi-fact-or-fiction-

Sonnenreich, W., J. Albanese and B. Stout (2006). Return On Security Investment (ROSI): A Practical Quantitative Model, http://www.infosecwriters.com/text_resources/pdf/ROSI-Practical_Model.pdf

Swanson, M. Nadya Bartol, John Sabato, Joan Hash, and Laurie Graffo (2003). Security Metrics Guide for Information Technology Systems, National Institute for Standards and Technology (NIST), http://www.rootsecure.net/content/downloads/pdf/nist_security_metrics_guide.pdf

II. Cyber-security Economics: State-of-the-Art

The economics of cyber-security (also termed economics of information security) applies principles of economics in order to analyse cyber-security. These principles encompass trade-offs that market players are facing, conducted under budgetary constraints. Moreover, the analyses also deal with government actions that either positively or negatively impact cyber-security, as explained in chapter I of this report.

This field of research not only uses economic theory to explain cyber-security problems, but is increasingly uses behavioural economics approaches. The origin of the link between the computer science and economics disciplines is attributed in the literature to Anderson (2001), who found that information insecurity is often due to misaligned incentives, rather than to the lack of suitable technical protections.[11] In this vain, security problems can be evaluated using concepts such as asymmetric information problems (moral hazard, adverse selection) or externalities. Many of the problems exist because of misallocated costs in terms of responsibility and liability for security incidents (Moore 2010). Thus, overview literature typically covers cybercrime statistics, market failures and instruments to improve market failures (see for example Moore 2010; Moore, Clayton and Anderson 2009). In Manshaei et al. (2013) an overview of game-theoretic models of cyber-security is provided.

Table 2 presents an overview of the different lines of research in the field of cyber economics. These range from micro-economic game-theoretical attacker-defender models to the modelling of market failures. Moreover, there is now also increasingly behavioural research.

Also very important is also the line of research that is devoted to the improvement of the statistical measurement and analysis of cybercrime costs. This in and of itself, is a difficult and tedious task as there are not many official authorities that compile statistics on cyber-crime.

There is the risk that more and more researchers use proprietary data in future, rendering studies that are neither transparent nor replicable, the very core of scientific objectivity. This risk is higher in the area of security research, where sensitive firm data sets are used (including Big Data).

Table 2 provides an overview of the field of cyber-economics with no claim of completeness. Roughly five areas can be differentiated: (1) game theoretical approaches modelling cyber-security problems, (2) experimental research (often also including game theory, but not always), (3) victim studies (using survey data or interviews), (4) methodological advances (focusing on measurement problems), and (5) other research that is not grouped with the other four. These works are also briefly described in Table 2.

Not listed are industry reports (see Appendix) from sources such as Symatec/Ponemon, Norton, McAfee, Verizon, Microsoft or Kaspersky Labs.

[11] The Economist “The weakest link”, http://www.economist.com/node/1389553

Table 2 Overview of the Research Field of Cyber-security Economics

Line of Research	Explanation	Authors
Game-theoretic Approaches to Cyber-security (incl. Discussions of Market Failures)		
Attacker-defender models	Weakest link game – security depends on the weakest link in the system (i.e. minimum effort)[12] Best shot game – System security depends on the maximum effort exerted Total effort game – System security depends on total effort of all participants Network games – Network economics of cyber crime	Böhme and Moore (2010); Grossklags et al. (2008a, 2008b); Johnson et al. (2011); Varian (2004); Nagurney et al. (2013)
Economics of Botnets	This research formalizes economic models of Botnets, i.e. the underground market for Botnets, where there is a demand and supply of Botnet services	Bensoussan et al. (2010); Li et al. (2008)
Cyber-insurance models	These works assess how cyber-insurance affects IT security and welfare of players, including conditions for taking on insurance. Other risk-sharing mechanisms among players are analysed as well	Shetty et al. (2010); Gordon et al. (2003a);
Security investment models	These papers analyse problems of interdependent security and characterize equilibria of rational players	Gordon and Loeb (2002); Kunreuther and Heal (2003)
Information sharing models	These works focus on how to improve cyber-security through sharing of critical incidence information among competitors	Gal-Or and Ghose (2005); Gordon et al. (2003b)
Experimental and Psychological Research (Action Research)		
Privacy breaches	This experimental research is related to breaches of consumer privacy simulated in the laboratory	Feri et al. (2016)
Behavioural cybercrime analytics	One article conducts the infiltration of an existing Botnet to analyse spam conversions. Other works focus on psychological characteristics of computer fraudsters or apply SN analysis of cybercrime (interviews of card fraudsters in forum)	Kanich et al. (2008); Rogers et al. (2006); Yip (2012)
Security decision-making	This research uses experiments in order to explore user behaviour with respect to security decisions or the response of users' security behaviour to framing	Caputo (2011); Grossklags et al. (2008b); Hess and Holt (2007); Rossof et al. (2013)
Victim Studies (incl. Psychological Research)		
Psychological impact of identity theft	This research uses interviews/surveys to study the patterns of identity theft as well as the financial and psychological impact on victims	Anderson et al. (2008); Pontell et al. (2008); Van Vliet and Dicks (2010)
Measurement of consumer reactions / vulnerability	These works are focused on the consumers perceptions and reactions to cyber-crime and surveys of who is vulnerable to fall for phishing	Böhme and Moore (2012); Sheng et al. (2010)
Methodological Advances		
Measurement of cybercrime*	These works are focused on the methodological question of how to measure cyber-crime	Anderson et al. (2012)
Other research		
Data breach notifications and share prices	These works concentrate on the impact of data breaches announced on the stock prices of companies	Cavusoglu et al. (2004); Campbell et al. (2003); Muntermann and Roßnagel (2009)

Notes: This literature overview notes works identified by the author, it is not a complete list of research works in the field. * The measurement of cybercrime is a topic of almost every industry report, these are not specifically listed here.

[12] The original papers are Hirshleifer (1983) and Van Huyck et al. (1990). Here, recent articles with a specific focus on information security are quoted.

2.1 Market Failures

Market failures exist where the free interplay of market forces fail to deliver an efficient allocation of resources, because prices are not reliable signals of supply and demand. The inefficiencies result in a loss of social welfare. Market failures are often attributed to information asymmetries, network externalities, public goods or natural monopoly. These will be discussed in the following. In the context of the adoption of PACS products and services, the problems discussed below have the potential to reduce the incentive to invest in technologies and procedures that improve cyber-security and privacy.

2.1.1 Information Asymmetries

Information asymmetries describe economic situations where market players act under conditions of incomplete information.[13] Such situations occur if one market side has more information than the other (e.g. in insurance) or where information is not available to market players in general. For example, it is widely known that there are only very little hard statistics on cybercrime and data breaches. Moreover, the institutions that report such statistics might have either an incentive to over- or under-report: "Without accurate information on online crime, it is hard for private markets to provide incentives for more secure software" (Moore, Clayton and Anderson 2009: 8). Three basic problems arise from information asymmetries: moral hazard, adverse selection and rationing (the latter is not discussed in this context). A lack of statistics on cybercrime and the damages caused by it leads to dealing with firms as well as consumer that have little incentive to invest in cyber-security, this includes the investment into innovative PACS technologies and procedures. These basic economic problems – in their extreme form – can either lead to the absence of markets or their break-down. In the chapter on instruments, remedial measures are discussed.

2.1.1.1 Adverse Selection and Signalling

Information asymmetries can lead to adverse selection problems (Akerlof 1970). These exist where an insurer only observes the average risk of the potential policyholder. He can then only set an average price for the insurance. Policyholders who are good risks (i.e., better than the average) in the pool will now cross-subsidize bad risks. They pay too much for the insurance policy considering that they are better than the average. In the case of risk-based pricing, the price for insurance would decline for this group of customers. This introduces dynamics whereby good risks opt out of insurance, while the bad risks remain in the pool, which will become unsustainable. Eventually, market breakdown can result.

Adverse selection problems are identified in software markets (Barnes 2004; Hahn and Layne-Ferrar 2007 arguing for a qualification of the argument), in electronic auction markets (Dewan and Hsu 2004; Huston and Spencer 2002), in online peer-to-peer lending (Lin et al. 2009) as well as in the context of privacy policies and trust seals (Edelman 2006; Vila et al. 2003).

[13] The following sections draw partially on U.S. Treasury Department (no date); Moore (2010) and Varian (2004).

Signalling problems result when firms face the challenge of signalling their cyber-security or privacy practices in a trustful and credible way to consumers. If such signals are credible, they provide differentiation power that influences a consumer's decision with respect to the purchase of a more secure product. If signalling (through trust marks and online seals) is possible it still bears the question, whether the signalled product quality is important enough that a sizable share of consumers will pay a premium for it. Signalling problems are part of some of the aforementioned literatures, including both Edelman (2006) and Vila et al. (2003) and for mobile application markets Akhawe and Finifter (2012) provide evidence. Edelman (2006) and Vila et al. (2003) explain that certification of trusted sides could attract those sites that are significantly less trustworthy. Additional misalignment of incentives could result if the certification authority does not bear the costs of wrongful signalling and is paid by the certification-seeking institution (ENISA 2013 and Jentzsch 2012).

One suggestion related to the lack of signals on information security is the proposal to issue information security ratings on service providers that are similar to credit ratings on firms (Zhou and Johnson 2009).[14]

2.1.1.2 Moral Hazard

The term "moral hazard" describes the situation, where a decision-maker does not have to bear all costs related to his or her behaviour. In the following, some examples are quoted that are relevant in the area of cyber-security.

Cyber-insurance: The information asymmetry arises between the insurer and the client. The client, say a firm in the financial services industry, has private information about how often it is attacked by hackers and how successful they are in terms of causing damage. The insurer does not have this information. Once the firm obtains cyber risk insurance, it could act more negligently (if not closely monitored by the insurer) because there would be coverage in case of data breaches.

Liability assignment: Another example in the area of the adoption of PACS products and services is liability. If there is no strict liability assigned (connected to punishment) for deficient software and/or programming mistakes, firms have an incentive to act carelessly about the security of the products they design. Downstream firms will only be able to buy deficient software. Moreover, if firms can externalize the costs of insecure software, they tend to under-invest in security.

Potential liability also plays a role for the voluntary adoption of sharing of critical incidence information among market players. One of the arguments is that such information shared could benefit competitors and that once data breaches become public knowledge liability to arise (U.S. Treasury Department, *no date*). This reduces the incentive to share critical infrastructure information.

[14] This line of research is primarily advanced by the Dartmouth Center for Digital Strategies in the U.S., http://digitalstrategies.tuck.dartmouth.edu/research/project-detail/adoption-of-risk-measures

2.1.2 NETWORK EXTERNALITIES

Most of the PACS technologies are network goods. The term describes goods whose utility depends on the number of users of said good. This is the case for telephones, emails, social networks, and certain software. The more that people use these products, the greater the positive externalities due to increased reachability and compatibility. Networks typically require the passing of a threshold of users (so-called critical mass), in order to develop non-linear growth. In this case a network can develop positive, but also negative externalities (such as clogging due to traffic congestion), which are typically not fully priced into the network services provided. Several problems are related to network goods, these are switching cists and technological lock-in as well as standards, as discussed in the following sections.

Switching costs and technological lock-in: Switching to a new security and privacy technology always bears the costs of purchase, implementation and learning, for example in the form of employee training. These costs can lead to lock-in of users, i.e., the continued use of a certain technology despite a better technological alternative. Moreover, sequential updates are common for systems and software creating path dependency. Technological incompatibility can also increase switching costs in aftermarkets (Garcia Mariñoso 2001).

It is important to note that switching not only depends on real, but also on perceived switching costs. These can be related to the user expectations of effort, money and time related to switching. While the increasing adoption of a new security technology is beneficial, a large user base of the older technology can act either as an entry barrier for the launch of products and, simultaneously, a new security technology might not be able to penetrate the market due to user inertia.

Box 2 Important Standards in the PACS Domain

(1) Security standards for products and services set by international standard setting bodies such as ISO standards.

(2) Standards of reporting of critical incidences (different private-sector initiatives such as VERIS), including data breaches.

(3) Standards for harmonized metrics for calculating risk premiums needs to be developed.

(4) Standardization of information about security ratings and privacy seals of firms needs to be developed.

Standards: Security and privacy standards might also act as market entry barrier. They might be too stringent or costly for innovative firms to achieve. Standards, on the other hand, have been proposed as a remedy for market failure (due to information asymmetry) related with low-quality of software (Moore 2013). Moreover, in order to credibly signal a higher security or privacy of a product or service to consumers, policymakers contemplate certification schemes. However, when considering these schemes they should require a minimum standardization of audit procedures and labelling. Otherwise a great variety of seals, labels and trust marks will emerge, which neither facilitates nor improves decision-making of consumers. An additional challenge connected with standards is coordination. If there is no coordination on specific standards such as standards for reporting security incidents and losses incurred from those, coordination failure can arise, resulting in a lack of reliable statistics.

2.1.3 PUBLIC GOODS

A public good is a good that is non-excludable and non-rival in consumption. To put it differently, it is difficult to stop others from using the products or service (such as excluding certain sailors from using a light-house as guidepost) and the consumption by one party does not exclude others from consumption (such as the informational content of a newspaper). With respect to cybersecurity and privacy, there are several problems connected:

Information as public good: Problems related to the public good features of information exist with respect to (1) personal privacy, (2) information sharing of critical information; and (3) cybersecurity research. Regarding personal data, the data breaches reported on almost a daily basis[15] show that it is difficult to exclude malevolent actors from data use.[16] With respect to information sharing, there is the tendency that, if no reciprocity mechanism is installed, participants free-ride on other's shared information. Finally, the benefits from research in cybersecurity and privacy in almost all cases cannot be fully privatized, if there are knowledge spill-overs that competitors can use for free. This leads to underinvestment in such research with negative effects on PACS innovation.

Security as public good: Information system reliability exhibits public good qualities. The party investing in security cannot fully internalize the returns on investment and therefore an under-provision of cybersecurity results. This is closely related to the below-discussed notion of "interdependent security" in economics, where there is a dependence on the actions of network participants.

2.1.4 NETWORK ECONOMICS AND INTERDEPENDENT SECURITY

In many instances, information systems are best characterized as networks. Networks consist of nodes and links, which can be the common adoption of software and systems or technological standards. However, networks can also consist of social interactions, such as information exchange, or mutual exposures that are related to financial or cyber-security risks. Network economics and social network analysis focus on such structures. The baseline assumption in this research field is that network formation and dynamics as well as structure have an impact on economic outcomes. If there is an outstanding characteristic of the cyber-security and privacy industry, it is the amplification of network externalities, as stated in the introductory part of this report.

Tipping point and non-linear growth: It is observable that the adoption of new technologies tends to follow a non-linear growth path, with non-linear growth happening after a specific threshold has been achieved and passed. Technology adoption can be driven by different forces, such as added value, social learning, but also social conformism (bandwagon effect) and other social interaction. Self-reinforcement may contribute to non-linear growth. Such growth paths can lead to market dominant positions of technology companies and a technologically homogenous environment.

[15] The source DataLossDB reports data breaches (http://datalossdb.org/)

[16] The problem resurfaces in another way in direct marketing, where it is difficult to exclude firms from unwanted use of information, which has led to the implementation of the Do-not-call-List in the U.S. (https://www.donotcall.gov/)

Path dependency – For network development, the decisions of the players in the past have an impact on future network structure. For example, the decision on the use of a specific platform creates switching costs that lead to inertia. A platform might be retained despite a better option being available.

Network externalities – Externalities are changes in utilities that are induced by other players' actions and that are not reflected in market prices (see also the discussion of the utility model in the chapter on privacy economics). For example, the use of a specific software can induce externalities, because the more users use it, its value increases.[17] There are direct externalities, which are directly attributable to an increase in diffusion and indirect externalities that arise with the production of complementary goods, technological nearness or learning effects.

Box 3 The Economics of Big Data Analysis

Big Data Analysis exhibits many network features discussed herein.

One important aspect is that many Big Data sets in the private sector are **mapping network activity** itself like in the telecommunications industry, energy industry (smart metering) and automobile industry (smart transportation applications). The analysis of this data represents a true challenge.

For consumer Big Data analytics can be **ambivalent**. While consumers might agree to data processing in the framework of the services sought, they are often not informed what inferences are made from their data. This can give rise to information externalities, positive or negative ones (further discussed in the chapter on privacy economics).

Positive externalities denote a positive change in utilities or payoffs, whereas **negative externalities** describe just the opposite. It is important to note that markets are not a well-suited mechanism to achieve social optimal levels of the provision of a good in the presence of externalities, because prices give the wrong signals. This again impacts on the inclination of market players to invest in innovative PACs.

Positive demand-side externalities describe the situation where the consumer's utility increases with increasing diffusion of, say, a technology. **Positive supply-side externalities** arise, where the increase diffusion of the product induces greater production of complementary goods, which in turn increases the value of the network for the network provider (i.e. the supplier).

Negative externalities can also arise on both sides of the market. Negative demand-side externalities may arise in information systems, because the insufficient incentive to invest in security by one market player can negatively affect the security of the others. This is one important aspect in Botnet economics, where people do not realize that insufficient protection of their computers can lead to involuntary participation in a Botnet.

While cooperation can often improve the situations described above, non-cooperative behaviour of players will often worsen the situation. For example, individual maximization of utility (by not investing in secure software to save on costs/time) can lead to socially sub-optimal outcomes resulting in system security failures or spread of Botnets.

[17] Metcalfe's Law states that the value of a network increases proportional to the square of the number of connected users.

In the economics literature, such security problems are formalized under the term of **interdependent risk**, where one central question is about investment incentives considered that the security risk magnitude also depends on other players' actions (Kunreuther and Heal 2003).

Complexity and network interaction can lead to tedious analytical problems. One of the main elements of networked economies is the interaction between several networks and, consequently, networks of networks. This gives rise to very complex problems that are analytically difficult if not impossible to solve. Complex dynamics of several connected networks, for example, may lead to the impossibility to predict an outcome due to several equilibria arising in economic modelling.

In complex networks systemic risk arises endogenously. It is the risk of negative spill-over effects that can cascade through shared links and therefore affect many network participants. Systemic risk is a function of the network structure (Burleson 2012). It describes a situation, where the actions of remote participants with whom only indirect links exist affect other parts of the network. Through increasing correlations among market players, the volatility in economic outcomes can increase due to social interactions, for example. One example includes cascade failures, where an attacked computer can be turned into an attacker (Greer 2003: 14) or become part of a Botnet. The **easier the propagation** of such attacks through the network, the more vulnerable it is. Moreover, complex systems are characterized by emergent vulnerabilities and behaviour, which that are currently under-researched.

2.1.5 NATURAL MONOPOLY

Another cause for market failure is the natural monopoly. The term denotes a specific cost structure that arises based on several conditions.[18] The cost structure typically leads to highly concentrated market structures with negative consequences for prices. Such conditions can be widely found in the IT industry as well as among IT services providers (such as Microsoft, Google, FaceBook and others). Prices might then reflect pricing power rather than demand fluctuations. In this case, they are not an informative signal to market players and do not lead to an efficient resource allocation.

Another problem that stems from market dominance in the IT industry is the homogeneous security culture. For example, it is argued that the Microsoft operating system dominance creates a harmful monoculture, where malware can spread more easily (Grady and Parisi 2006, Greer 2003). Therefore, cyber-diversity (in platforms) should be advanced in the IT ecosystem or should be the goal of system architecture. This argument is borrowed from nature, where some authors state that the richest ecosystems are the most diverse ones (Greer 2003: 14). Moreover, others argue that monoculture creates the incentive for attack, because the results are more spectacular, the more actors are hit. Again, individual utility maximization can lead to sub-optimal results: While security of the Internet could benefit from increased diversity, individuals have incentives for monoculture (Stamp 2004: 120).

[18] These are: sub-additivity, economies of scale (ESA) and scope (ESO) as well as sustainability. For the first to be present, the long-term average costs (LTAC) decrease and the marginal costs (MC) are below the LTAC. For ESA it holds that there are high fixed costs, LTAC decrease and MC are small. Moreover, ESO describe situation where bundling is cheaper and individual production and finally sustainability describes a situation, where there is free entry and no sunk costs.

Unfortunately, we currently lack empirical proof that diversity in comparison to technology monoculture increases cyber-resilience. Moreover, the diversity argument comes at the cost of standardization, which proves to have great advantages. In addition, shared vulnerabilities can be more easily patched across many computers. The advancement of cyber-diversity could induce hackers to develop more complex viruses, which are poly- and metamorphic and therefore more difficult to detect (Stamp 2004: 120). The trade-off between diversity and standardization is studied by Chen et al. (2011) who model downtime loss of a firm as function of (a) investment in security technologies; (b) software diversification to limit the risk of correlated failure; and (c) investment in IT resources to repair failures due to attacks. This analysis shows under what conditions the diversification strategy is advantageous (this is not further discussed in this report, the interested reader is referred to the referenced work).

Future research topics in the area of PACS economics: In order to enable a better understanding of how the different deficiencies (such as information asymmetries) impact on PACS adoption and bias incentives, research ought to focus on:

- Better tools to enable network analysis and the analysis of contagious security incidents and their costs (to players and the economy);
- Behavioral research in the economics of cyber-security ought to be strengthened and the position of researchers conducting such research ought to be clarified in terms of potential legal liability;
- Better technique to allow for the elicitation of vulnerability factors and resilience factors must be developed; and
- Techniques such as ratings and information sharing on risks of firms ought to be better explored. If the IT security risk of firms becomes public knowledge, there is a greater incentive to invest in security technologies.

References to Chapter II

Akerlof, G. A. (1970). The Market for "Lemons": Quality Uncertainty and the Market Mechanism, Quarterly Journal of Economics 488: 489–490.

Akhawe, D. and M. Finifter (2012). Product Labels for Mobile Application Markets. Mobile Security Technologies Conference, San Francisco, CA USA, 2012, devd.me/papers/mobile-metrics.pdf

Anderson, R. (2001). Why Information Security is Hard—An Economic Perspective. Proceedings of the 17th Annual Computer Security Applications Conference, 358–65. IEEE Computer Society.

Anderson, R., C. Barton, R. Böhme, R. Clayton, M. van Eeten, M. Levi, T. Moore, and S. Savage (2012). Measuring the cost of cybercrime. WEIS 2012 presentation.

Anderson, K.B., E. Durbin, and M.A. Salinger (2008). Identity Theft. *Journal of Economic Perspectives* 22 (2), 171–192.

Barnes, D. (2004). Deworming the Internet, in: Texas Law Journal 83 (279): 279–329.

Bensoussan, A., M. Kantarcioglu, C. H. SingRu (2010). A Game-Theoretical Approach for Finding Optimal Strategies in a Botnet Defense Model. Decision and Game Theory for Security, Lecture Notes in Computer Science Volume 6442, 2010, pp. 135-148.

Böhme, R. and T. Moore (2012). How do consumers react to cybercrime? In *APWG eCrime Researchers Summit (eCrime)*, October 2012.

Böhme, R. and T. Moore (2010). The iterated weakest link. *IEEE Security & Privacy*, 8(1): 53-55.

Burleson, W. (2012). Cybersecurity Risk Analysis and Investment Optimization, ACSC 2012 Prim-the-Pump Project Update Nov 15, 2012, UMass Amherst, http://www.acscenter.org/news-events/wayne_burleson.pdf

Byung Cho, K., P. Chen and T. Mukhopadhyay (2009). An Economic Analysis of the Software Market with a Risk-Sharing Mechanism, *International Journal of Electronic Commerce* 14(2): 7-39, http://www.law.harvard.edu/students/orgs/jlpp/Vol30_No1_Hahnonline.pdf

Campbell, L. Gordon, M. Loeb, and L. Zhou (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. Journal of Computer Security, 11(3): 431–448.

Caputo, D.D. (2011). Leveraging Human Behavior to reduce Cyber-security Risk: Spear-fishing Study Design, Results and Discussion, Presentation, http://www.thei3p.org/docs/events/humanbehaviourworkshop1011/deannaspearphishing.pdf

Cavusoglu, H., Mishra, B.& Raghunathan, S. (2004). The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. International Journal of Electronic Commerce, 9(1): 69 – 104.

Danezis, G., Cvrcek, D., M. Kumpost, V. Matyas, (2005). A Study on the Value of Location Privacy, http://www.fi.muni.cz/usr/matyas/PriceOfLocationPrivacy_proceedings.pdf

Dewan, S. and V. Hsu (2004). Adverse Selection in Electronic Markets: Evidence from Online Stamp Auctions, *Journal of Industrial Economics*, LII(4):497–516.

ENISA (2013). On the security, privacy and usability of online seals – An overview, https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/on-the-security-privacy-and-usability-of-online-seals/at_download/fullReport

Edelman, B. (2006). Adverse Selection in Online 'Trust' Certifications. Fifth Workshop on the Economics of Information Security 2006, http://weis2006.econinfosec.org/docs/10.pdf

Feri F., C. Giannetti, and N. Jentzsch (2016). Disclosure of Personal Information under Risk of Privacy Shocks, Journal of Economic Behavior and Organization, 123 (March): 138–148.

Gal-Or, E. and A. Ghose (2005). The Economic Incentives for Sharing Security Information, *Information Systems Research* 16(2): 186–208.

Garcia Mariñoso, B. (2001). Technological incompatibility, endogenous switching costs and lock-in, *Journal of Industrial Economics* 49: 281–298.

Gideon, J., Cranor, L., Egelman, S. and Acquisti, A. (2006) 'Power Strips, Prophylactics, and Privacy, Oh My!', Institute for Software Research (Paper 24), http://repository.cmu.edu/isr/24

Gordon, L.A., Loeb, M., Sohail, T. (2003a). A framework for using insurance for cyber-risk management. *Communications of the ACM* 46(3), 81–85.

Gordon, L.A., M.P. Loeb (2002). The economics of information security investment. *ACM Transactions on Information Systems Security* 5(4), 438–457.

Gordon L.A., M.P. Loeb and W. Lucyshyn (2003b). Sharing information on computer systems security: An economic analysis. *Journal of Accounting and Public Policy* 22(6): 461–485.

Grossklags, J., N. Christin, J. Chuang (2008a). Predicted and Observed User Behavior in the Weakest-Link Security Game. Proceedings of the 2008 USENIX Workshop on Usability, Psychology, and Security (UPSEC'08), April 2008.

Grossklags, J., N. Christin, J. Chuang (2008b). Secure or Insure? A Game-Theoretic Analysis of Information Security Games. Proceedings of the 17th International World Wide Web Conference (WWW'08), April 2008.

Hahn, R.W., A. Layne Farrar (2007). The Law and Economics of Software Security, *Harvard Journal of Law and Public Policy* 283 (2006-2007), http://www.law.harvard.edu/students/orgs/jlpp/Vol30_No1_Hahnonline.pdf

Haley, K.J., and Daniel M., T. Fessler (2005). Nobody's Watching? Subtle Cues Affect Generosity in an Anonymous Economic Game. Evolution of Human Behavior, 26(3): 245–56.

Hess, R., C. Holt, and A. Smith (2007). Coordination of strategic responses to security threats: Laboratory evidence. *Experimental Economics*, 10(3):235-250.

Hirshleifer, J. (1983). From Weakest-Link to Best-Shot: The Voluntary Provision of Public Goods, *Public Choice* 41(3): 371–86.

Huston, J.H. and R.W. Spencer (2002). Quality, Uncertainty and the Internet: The Market for Cyber Lemons*, The American Economist* 46 (1): 50-60.

Hui, K., Teo, H., Lee, S. (2007). The value of privacy assurance: An exploratory field experiment. Mis Quarterly 31 (1), 19–33.

Jenni, K.E. and G. Loewenstein (1997). Explaining the 'Identifiable Victim Effect.' Journal of Risk and Uncertainty 14(3): 235-257.

Jentzsch, N. (2012). Was können Datenschutz-Gütesiegel leisten? *Wirtschaftsdienst* 92 (6): 413-419, http://link.springer.com/article/10.1007/s10273-012-1397-9?no-access=true

Johnson, B., J. Grossklags, N. Christin, J. Chuang (2011). Nash Equilibria for Weakest Target Security Games with Heterogeneous Agents. Proceedings of the 2nd International Conference on Game Theory for Networks (GameNets 2011), April 2011.

Kanich, C., C. Kreibich, K. Levchenko, B. Enright, G.M. Voelker, V. Paxson, S. Savage (2008). Spamalytics: An Empirical Analysis of Spam Marketing Conversion. P*roceedings of ACM Conference on Computer and Communications Security* (CCS), 3–14. ACM Press.

Kunreuther, H. and G. Heal (2003). Interdependent Security, *Journal of Risk and Uncertainty* 26 (2-3): 231-249.

Li, Z., Q. Liao, A. Siegel (2008). Botnet Economics: Uncertainty Matters, Workshop on the Economics of Information Security, http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.139.7141

Lin, M., N.R. Prabhala and S. Viswanathan (2009). Judging Borrowers by The Company They Keep: Social Networks and Adverse Selection in Online Peer-to-Peer Lending, http://ssrn.com/abstract=1355679

Manshaei, H., Q. Zhu, T. Alpcan, T. Basar, J.P. Hubaux (2013) Game Theory Meets Network Security and Privacy, ACM Computing Surveys (CSUR), Volume 45 Issue 3, June.

Muntermann, J. and H. Roßnagel (2009). On the Effectiveness of Privacy Breach Disclosure Legislation in Europe: Empirical Evidence from the US Stock Market, NordSec '09 Proceedings of the 14th Nordic Conference on Secure IT Systems: Identity and Privacy in the Internet Age, pp. 1 – 14.

Mukhopadhyay, A., S. Chatterjee, D. Saha, A. Mahanti, S.K. Sadhukhan (2013). Cyber-risk decision models: To insure IT or not? *Decision Support Systems* 56: 11-26.

Moore, R. (2013). Standardisation: A tool for addressing market failure within the software industry, *Computer Law & Security Review* 29(4): 413 – 429.

Moore, T. (2010). The economics of cyber-security: Principles and policy options. In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*. The National Academies Press.

Moore, T., R. Clayton, and R. Anderson (2009). The economics of online crime. *Journal of Economic Perspectives* 23(3): 3-20.

Muntermann, J. and H. Roßnagel (2009). On the Effectiveness of Privacy Breach Disclosure Legislation in Europe: Empirical Evidence from the US Stock Market, in: Lecture Notes in Computer Science , A. Jøsang, T. Maseng and S. Knapskog (eds.), Springer Berlin / Heidelberg, 1-14.

Nagurney, A., Wayne Burleson, Mila Sherman, Senay Solak, and Chris Misra (2013). Network Economics of Cyber Crime with Applications to Financial Service Organizations, University of Massachusetts Amherst, Massachusetts 01003, INFORMS Annual Meeting, Minneapolis, Minnesota, October 6-9, 2013, http://supernet.isenberg.umass.edu/visuals/INFORMS_Cybercrime_Nagurney.pdf

Norberg P.A., D.R. Horne, and D.A. Horne. 2007. "The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors" The Journal of Consumer Affairs, 41(1), 100-126.

Pontell, H.N, G.C. Brown, A. Tosouni (2008). Stolen Identities: A Victim Survey. *Crime Prevention Studies*, 23, pp. 57-85.

Rifon, N.J., R. LaRose, S. M. Choi. Your Privacy is Sealed: Effects of Privacy Seals on Trust and Personal Disclosures, Journal of Consumer Affairs 39 (2005), Nr. 2, S. 337-360.

Rogers, M.K., K. Seigfried, K. Tidke (2006). Self-reported computer criminal behavior: A psychological analysis, *Digital Investigation* 3: 116-120.

Rosoff, H., Cui, J., Richard J.S. (2013). Heuristics and biases in cyber-security dilemmas. *Environment Systems and Decisions* 33 (4): 517–529.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. Proceedings of the 28th International Conference on Human Factors in Computing Systems, pp. 373-382, http://lorrie.cranor.org/pubs/pap1162-sheng.pdf

Shetty, N., G. A. Schwartz, M. Felegyhazi, and J. Walrand (2010). Competitive cyber-insurance and internet security, in T. Moore, D. Pym, and C. Ioannidis, editors, Economics of Information Security and Privacy, pp. 229-247, Springer-Verlag.

Van Vliet, K., and J. Dicks (2010). The psychological impact of identity theft: Preliminary findings of a qualitative study. Mimeo, University of Alberta.

Van Huyck, B., R.C. Battallio and R.O. Beil (1990). Tacit coordination games, strategic uncertainty, and coordination failure. *American Economic Review* 80(1): 234–248.

Varian, H. (2004). System Reliability and Free Riding. In Economics of Information Security, L.Jean Camp and Stephen Lewis (Eds.). Advances in Information Security, Vol. 12. Springer, 1–15.

Vila, T., R. Greenstadt, and D. Molnar (2004). Why We Can't be Bothered to Read Privacy Policies: Models of Privacy Economics as a Lemons Market. In The Economics of Information Security, L.J. Camp and S. Lewis, eds., Kluwer, 143–154. http://www.cpppe.umd.edu/rhsmith3/papers/Final_session3_molnar.greenstadt.vila.pdf

Yip, M., N. Shadbolt, T. Tiropanis and C. Webber (2012). The digital underground economy: a social network approach to understanding cybercrime. In: Digital Futures 2012 - The Third Annual Digital Economy All Hands Conference, Aberdeen, GB, 23 - 25 Oct 2012.

Zhen L., Q. Liao and A. Striegel (2009). Botnet Economics: Uncertainty Matters, Managing Information Risk and the Economics of Security, pp 245-267.

Zhou, Z.Z., E. Johnson (2009). The Impact of Information Security Ratings on Vendor Competition, Center for Digital Strategies, Mimeo, weis09.infosecon.net/files/134/paper134.pdf

III. Economics of Privacy

Many problems that arise in relation to the intermediation of personal data in markets are rooted in the peculiar character of personal data and the difficulty to keep it private. Personal data can be treated as an economic good. However, it may also constitute a property of an economic transaction. To make matters even more complicated, not revealing information might also have effects on privacy. In situations with a limited number of good and bad types of players not acting may reveal something about a player's type.[19] These basic aspects give rise to complex economic problems. The first to notice that privacy constitutes an interesting problem also from an economists' perspective were Hirshleifer (1971, 1980), Stigler (1980) and Posner (1981). With respect to personal data as economic good, a number of properties have been known for a quite a while, while others only now come to the forefront, especially with the evolution of Big Data. This will be discussed in greater detail below.

As stated in the introduction of this report, the economics of (personal) privacy is related to actions of an *identified or identifiable individual* who can be singled out from an anonymous mass. The economics of privacy focuses on incentives and actions of firms and consumers with respect to personal data and the ambiguous welfare effects arising from their disclosure. Researchers in the field focus on the cost-benefit trade-offs of actors, their strategic actions, market outcomes and market failures, similar to cyber-security economics. The research increasingly converges with mechanism design[20] and differential privacy, where mechanisms are developed that have certain appreciated properties.[21]

3.1 The Economic Concept of Personal Information

The current legal definition of personal information is stated in Article 2 of the EU Data Protection Directive:

> *(a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;*

This definition clearly states that personal data must be *related to an identified or identifiable natural person*. This view is also employed in this report. However, the economic concept of personal data adds further aspects by putting it into the context of market intermediation. Compared to traditional goods personal data is described as "intangible asset" (OECD 2013: 10), which consists of the following properties:

[19] Consider a situation, where there are only two types of players, one with high and the other with low credit risk. If low risks have an incentive to reveal their risk truthfully in a transaction and do so, they automatically reveal the other as high risks (Hermalin and Katz 2006).

[20] Mechanism design is a part of economic theory that seeks solutions on interaction mechanisms in markets that improve market allocations.

[21] Differential privacy is another development related to mechanism design. This theory seeks to find mechanisms, where agents can some information in private (see section 3.8.4 in this report).

- **Intangibility:** personal information is not bound to a specific medium, but can be stored in different media;
- **Non-rivalry:** If one person consumes the information, the informational content is not reduced and another person can consume it as well. Information is not a scarce resource in itself, but the material it is bound to is scarce;[22]
- **Non-excludability:** Once information is produced (collected), it is difficult to exclude others from using it;
- **Identity-relation:** Personal information reveals either completely or partially the identity of its subject. It then introduces psychological effects that alter the utility function of individuals compared to standard situations under anonymity;[23] and
- **Information externalities:** The combination of different pieces of information (name, gender, date of birth, place of living) can give rise to inferences (about income, etc.). Moreover, externalities exist, where the revelation of others impact on an individual's welfare.

These properties give rise to a number of problems once information is traded in a market environment. In addition, these properties make the good "personal data" rather special. In fact, most of the diagnosed market failures in the economics of cyber-crime, resurface in the economics of privacy and vice versa. This will be discussed in greater detail below. On the outset of the research overview, two additional distinctions need to be made (see Jentzsch et al. 2012):

> ***Private information*** denotes an unequal *distribution of information* among market players (e.g. consumers and firms), where one player holds information that the other does not have. Therefore, information is private if it is not common knowledge. "Private" describes a property of the information distribution.
>
> ***Personal information*** denotes *differentiation power of information*, which allows a single person to be identified out of the mass. This singling-out from the mass is based on a sampling probability. If the probability of drawing the person from the mass is 1 based upon the selected identifier the individual is uniquely identified. Therefore, 'personal' describes a property of personal information itself and not of the distribution of personal data.

Economic Concept of Personal Privacy: The state of personal privacy arises with an asymmetric distribution of personal information between market participants, where one side *privately* holds personal information. Privacy is therefore a relationship of asymmetric distribution of personal data between market players. Other definitions might exist, in the domain of philosophy or in the juristic domain, but these are not subject of research here.

Different types of personal data must be differentiated, because they give rise to different types of information asymmetries associated with them (for the **Table 3** see also OECD (2013) with additions by the author).

[22] Most of standard economics deals with situations of allocation of resources that are scarce.

[23] For example, while the sale of personal data can be welfare-enhancing in an economic sense (as money can be earned from disclosure), individuals might find it reflects negatively on their reputation and therefore refrain from selling it (which would maximize their social welfare), see Jentzsch (2014).

Table 3 Different Types of Personal Data

Volunteered Data	Observed Data (Traffic Data)	Inferred Data
Individuals disclose the data directly to the party collecting it	Observed data is produced as by-product of using information technologies & associated online services	Inferred data is additional information arising from the analysis of personal data.
Social networks, online registrations, writing of commentaries or rating quality of books, service providers, etc.	Call logs and location data in mobile telephony, Internet behaviour, etc.	Behavioural & social scoring, social graphs, crowd monitoring, social multiplier, Big Data applications, etc. De-anonymization of anonymized data
Disclosure is actively provided by data the subject and collection therefore is obvious	Collection and storage are often less obvious for data subject	Type and extent of analysis as well as its outcome is often wholly unknown to the data subject
No information asymmetry	Information asymmetry	Deep information asymmetry

Source: OECD (2013), with additions by the author.

Volunteer data, observed data and inferred data are interrelated. In many transactions, all three exist. However, while in the volunteered case it is often clear to the individual what data are shared, this is not the case for observed or traffic data. Here many individuals have a "suspicion" or a "feeling" that such data is collected, but not a deeper understanding. In many situations the comfort of quick communication (or pre-filled forms) outweigh privacy considerations. This is where consumer education is fairly important, i.e. greater education beyond consent. Finally, in the case of inferred data, the analysis techniques as well as the results are often wholly unknown for individuals.[24]

Another dimension of insight about individuals is delivered by Big Data. Big Data sets are characterized by the three Vs: volume, velocity, and variety. Big Data sets are not only large, exceeding conventional computing and analysis power by containing millions of information items on persons, but they are also unstructured. In addition, these sets are fast-moving, some even being real-time. These sets allow identification of new effects. One example of such an analysis is the identification of the so-called social multiplier. The multiplier is an effect in the network that is not driven by exogenous factors of network participants (age, gender) or common shocks to them (price reductions), but endogenous social interaction in the network.

However, from a theoretical point of view it is not the largeness of datasets that proves to be problematic, but the network character of the data, which needs to be described and analysed with

[24] In a recent case in Germany, the German Bundesgerichtshof decided that the credit reporting agency SCHUFA does not have to disclose the calculation of its score, as the latter is considered to be a trade secret, http://www.zeit.de/wirtschaft/2014-01/schufa-bgh-urteil-bonitaet-berechnung-auskunft

new techniques in order to be able to extract the effect of network structure or dynamics on economic outcomes.

3.2 Research Overview

In the following, an introductory overview of the current research landscape in the economics of privacy is given. This overview is not intended to be complete and only provides a guide for the interested reader where to look for more information. The research works discussed herein also potentially enable a better understanding why some of the business innovations in the area of PACS do not work. Start-up problems for new business models in personal data markets might be associated with:

- A limited understanding of "mechanisms" of markets for personal data; and/or
- A limited understanding of the economic incentives of market participants involved in information trade.

One suggestion for PACS developers, firms and other stakeholders is to study the outcome of research conducted in the area in order to develop a better understanding of the problems, they will be confronted with when offering new services or products. The same is recommendable for policy makers who want to facilitate economic activity in the area and who want to avoid costly and ineffective incentive schemes. To date, the economics of privacy has developed a diverse research field with different approaches employed and methods applied, where any taxonomy is necessarily somewhat incomplete.

3.2.1 Basic Concepts and Insights

In order to understand the subtleties of the economics of privacy, one needs to start with basic definitional and conceptual work, such as the type of transaction and the types of players involved. In the first step it must be understood what types of transactions is the subject of the research. Is it a pure information transaction (IT) or a composite transaction that consists of a good and information transaction (GT + IT) running in parallel? Figure 4 shows these two types:

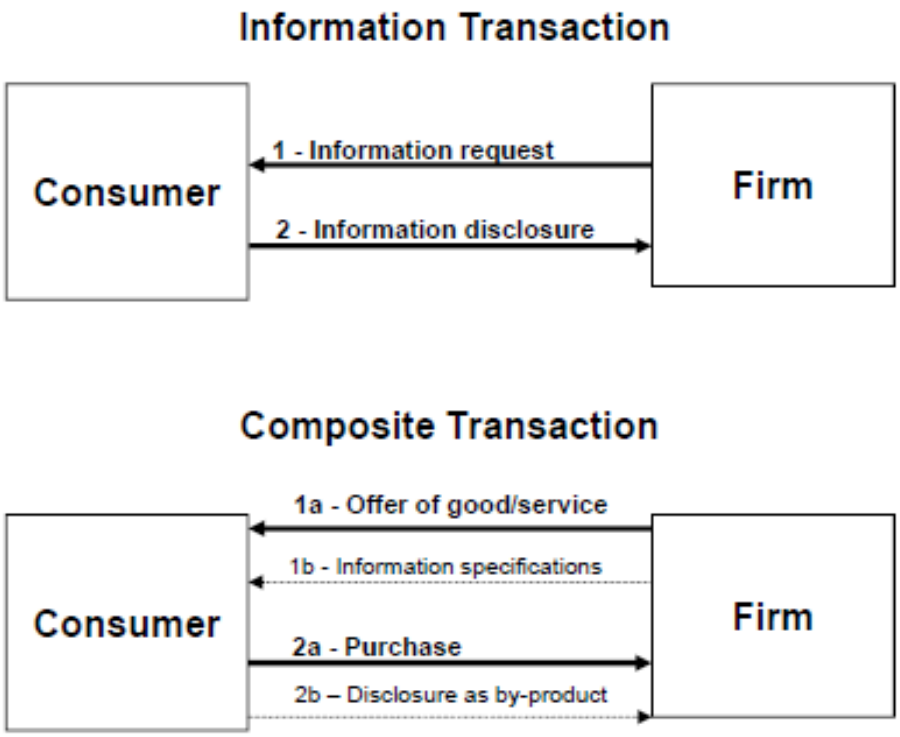
- **Information transaction (IT):** Here, only information is exchanged. The exchange is either incentivized with money or a social exchange, where the incentive is reciprocity. Examples are Google, Facebook, Twitter and marketing surveys; and

- **Composite transaction (GT+IT):** The main exchange is that of a good or service (1a and 2a in Figure 4). However, there is also an implicit information transaction that takes part in parallel (1b and 2b in Figure 4). Composite transactions can give rise to salience (Della Vigna 2006). Examples include online purchases of goods, banking and insurance transactions conducted online.

In the first type of transaction only information is exchanged between primary transaction partners, examples are surveys by marketing companies, the use of Internet search engines, and online cloud services that are "for free." In these transactions, pointing back to the volunteered data in **Table 3**

above, the exchange is rather obvious to the data subject involved.

Figure 4 Information and Composite Transaction



Source: Jentzsch et al. (2012).

In a composite transaction, however, the focus of the consumer is often on the good/service exchanged, such as the book, DVD or insurance to be purchased (see **Figure 4**). The focus is not on the personal data exchanged as by-product to the main transaction. If salience comes into play, the cost-benefit trade-off of the data exchanged enters the utility function of the consumer with a lower weight (in Della Vigna 2009 a general notion of salience is discussed). In addition, the disclosure of personal data could be simply a property of the transaction, which is often ignored by the consumer or he/she is unaware of it.[25]

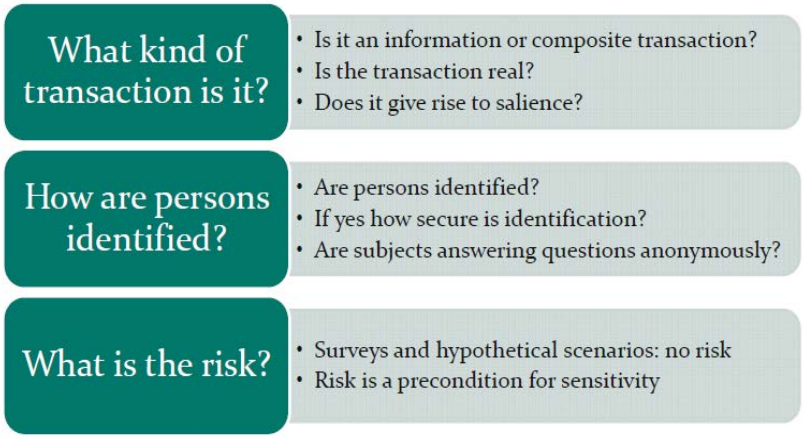
Information exchange can also alter the expected value of a product or service in the next period, if personalization takes place. To make matters more complicated, there is in many cases a succession of the above. Consider the Google business model, where first information is collected based upon social exchange (IT) and then services based upon these data are sold to third parties (incentivized IT).

In a second step, it must be differentiated between works that apply **secure personal**

[25] For example, compare payments made in cash or with payments made by credit cards (Gold, Platinum) that allow inferences about the financial strength of a person. The same holds for making online purchases using an Apple Macintosh computer.

identification[26] and works that do not apply such. These two work streams can be regarded as complementary to each other, rather than rivalries. There are a wide variety of economic transactions based upon different identification techniques. Compare, for example, the opening of a bank account with the use of free emails services on the Internet, where banks are subject to international due diligence standards set by the Financial Action Task Force on Know-Your-Customer. Free Internet email services, however, do not apply the same right in identity checking as banks do. **Figure 5** shows this differentiation.

Figure 5 Privacy Economics: Research Differentiation



Source: The author.

Research not using secure identification is often survey-based or uses hypothetical scenarios. The problem is that we do not learn much about actual behaviour from hypothetical scenarios, because there is no or only very weak correlation with actual behaviour (Krahnen et al. 1997). In experimental economics, individuals typically act in the laboratory under the condition of anonymity. From these experiments we learn little about personal privacy.

In the next section, it is elaborated on the market failures that are associated with the trade of goods that contain personal data. As a disclaimer it must be stated that the research discussed herein is different from works in economics on social identity and self-categorization (Akerlof and Kranton 2000; Benjamin et al. 2010).[27] This strand diverges away from the main topic of interest.

3.2.2 Market Failure Problems

In the following, the most important problems relating to market failures in the intermediation of personal data are discussed. It must be noted that the challenges surfacing here are very similar to those in the economics of cyber-security.

[26] With secure personal identification a visual check by common ID means such as official ID cards is meant.

[27] Akerlof and Kranton (2000) state that if there is conformity to a specific group with which the subject identifies, it increases a subject's utility.

3.2.2.1 Information Asymmetries

As stated in the chapter on cyber-security economics, market players act under conditions of incomplete information. With regard to personal information, it is the data subject holding private information on her/himself that the transaction partner does not have. This may be either information about his/her type or information about his/her actions (which reveal in many cases the type). What is important is that this private information is payoff-relevant: If it is not payoff-relevant, no strategic interactions will arise. Payoff-relevant information includes:

- **Identity information:** Identity information is the pre-condition for the emergence of personal information. We apply a broad concept here, including technical identifiers, such as IP addresses. What is important is whether the identifier allows the individual identification with a high probability, whether it allows authorization and re-identification of individuals and with it personalization of services and price discrimination.

- **Type information:** This information is based upon identification and reveals payoff-relevant traits in an individual. Examples include borrower creditworthiness, worker productivity and a buyer's valuation of a good.[28] This type of information allows a *rank-ordering of individuals* (so-called vertical information). Once the data subject is sophisticated, it can foresee the impact type-revelation will have on the expected payoff. Thus, there is a specific extrinsically motivated sensitivity related to the disclosure of such information.

- **Preference information:** This type of information is related to **personal preferences**, which *does not automatically induce a rank-ordering of individuals* (so-called horizontal information).[29] Examples are preferences for specific colors or shapes. If preference information is not payoff-relevant, no sensitivity is associated with it.

Let us now look at type information: Assume that a payoff-relevant trait is a latent variable that cannot directly be observed, δ (e.g. creditworthiness of a person). The person decides to send signal $\hat{\delta}$ to the other market side, e.g. a bank. The other party now must build an expectation about quality of the signal, i.e. whether $\hat{\delta} = \delta$. In order to be informative the signal must be highly correlated with the individual's type and should not be easy to manipulate.

The model formalizing this problem is called signaling game. In these games, the player with the private type information can decide whether to invest effort in a signal. The player wants to send out a signal that maximizes his/her payoff. It is important that in these games, three types of equilibria may arise: **pooling equilibriums, separating equilibriums and semi-separating equilibriums**. A **pooling equilibrium** characterizes the situation where all players choose the same signal, independent of their type. In a **separating equilibrium**, the players choose a signal that differentiates them from the other types. In the **semi-separating equilibrium,** there are more types than signals and these types pool on specific signals. Once there is vertical type information and the better-ranked type can maximize payoff by credibly revealing private information, there will be full revelation of all types in equilibrium (Hermalin and Katz 2006). One consequence is that there will be

[28] While in some cases, it can be assumed that nature draws the type (such as an applicant's intelligence), in others, an action is subject to strategic behaviour (such as paying off loans to keep a good credit score).

[29] See also Stole (2007) and Jentzsch et al. (2013) for the different types of competitive effects of such information.

no unique market-clearing price anymore, because now a different price can be charged to each different type. The net welfare effects depend on the set-up of the model.

In future, **Big Data analysis** as well as **data combination from different sources** will allow firms to drastically reduce the pre-existing information asymmetries associated with consumers. Behavioral or social scoring or other predictive modeling is the analytical tool that helps to build expectations about the future behavior of individuals. The currently existing information asymmetries might change in a way that enables firms to infer the type of a consumer, *before the consumer has decided to disclose his private information* for the simple reason that the firm can make inferences from similar types and their behavior. Disclosure of private information in this case would not be a strategic decision variable of the consumer anymore, as the admittance of type recognition is taken out of the consumer's hand and choice. Moreover, there will no option of strategic information manipulation anymore except for the very special case where a consumer knows what a firm collects and how it analyses the data. Informational rents obtained by the consumer from strategically deciding about type disclosure will disappear.

Of course, the large-scale data collections on individuals will, at the same time, avert problems such as moral hazard or adverse selection. These effects are widely known and have been studied intensively in the past in the economic literature.

3.2.2.1 Public Goods

As discussed at length, information has features of a public good, which can only partially be modified by specific precautions. Imperfect security will always lead to data leakages. Moreover, the characteristic of non-rivalry may lead to the use and exploitation of personal data by many different market players. Seen from a competitive angle once two competitors compete on the same information, personalization can reduce the firms' differentiation just as price discrimination leads to more intensified competition (Zhang 2011).

3.2.2.2 Information Externalities

The standard unraveling argument illustrates how disclosure actions by a single individual can affect other parties without mutual agreement and compensation. In many instances, individuals do not take such externalities into account when deciding upon personal data disclosure. These externalities can have a positive or a negative impact on the other individuals' welfare. In essence, information externalities represent social costs:

- A **positive information externality** leads to an increase in an individual's utility from information disclosed by others. Examples are more precise recommender systems online or better fitting personalized products; but

- A **negative information externality** exists, when the disclosure of information by others negatively affects the utility of an individual. Examples are voluntary submissions of genetic or blood tests to insurance firms (Rothschild and Stiglitz 1997) as well as voluntary drug tests by employees. Individuals declining participation may signal a negative trait.

The standard unraveling argument holds that giving up personal and private information also affects the privacy of other individuals as these are interdependent problems (so-called "privacy

externality"). The inter-dependent information relating to multiple transaction parties as been termed "multiple subjects' personal data" (Gnesi et al 2014).

One remedy to the privacy protection problem identified is by giving individuals greater property rights over their personal data (Sholtz 2001; Jentzsch 2007). These property rights include the right to opt-in, to access information, to have it corrected and erased if necessary, among other rights. Such an approach may help internalize the negative externalities that are primarily associated with the exploitation of personal data by companies. But as we now know, there are many other types of transactions. Moreover, in many circumstances this approach can work, the unraveling argument (Hermalin and Katz 2006) suggests a complete ban of information disclosures in order to effectively stop unraveling in markets. This might be the workable approach in very sensitive areas, but is certainly not practical for common services such as telecommunication and banking, where discrimination is efficient up to a certain point.

In fact, the presence of externalities of voluntary information disclosure represents a difficult problem for policymakers (Jentzsch 2014). It seems most logical to combine approaches in order to effectively increase the protection of privacy if this is a societal goal. For example, in critical areas such as insurance, the action would be to forbid insurers from obtaining genetic code from individuals.[30]

Box 4 Information Externalities and Pricing

Externalities arise in a situation where the action of an individual has an impact on another individual's welfare and there exists no mutual agreement of compensation between the parties.

Parties that place negative externalities onto other parties externalize part of the costs of their actions. Thus, prices do not fully reflect social costs associated with the respective action.

Such inefficiencies can be reduced through specification of liability or facilitation of compensatory rules.

3.2.2.3 Network Externalities

As much of the personal data collected and analyzed today stems from different sources connected by a network, much of what was discussed in the section on Network Economics also holds here. Modern advertisers compile personal data from multiple firms selling to consumers, credit reporting agencies collect data from a host of financial service providers and consumers directly share information over social networks. Such networks can lead to an increase of switching costs as well as to lock-in (if switching is prohibitively costly). One example is social networks. The inability to transfer the personal profile from one site to another (maybe less privacy-invasive) network paired with the increased utility of having all friends in the same network render persistent market dominance of one main provider.

In general dominance enables a firm to determine prices and control production in a given market. The production cost structure in digital markets almost inevitably renders dominant players. The access to personal data of users increases the barrier to entry for new competitors as personalization can lead to lock-in. Thus, this could harm consumer welfare. In the following, we concentrate on the empirical work and exclude theoretical work on the economics of privacy. The interested reader is referred to Jentzsch et al. (2012: 13) for a brief introduction to some theoretical papers.

[30] Employers and health insurers are not allowed to obtain results of genetic testing. This refers to the Genetic Information Non-discrimination Act of 2008 in the US.

3.2.3 EMPIRICAL WORKS ON PRIVACY (SURVEYS AND EXPERIMENTS)

The origin of the experimental economics of privacy are works that modify one variable in standard games (such as the Dictator Game, Trust Game, Ultimatum Game, Prisoner's Dilemma, Public Goods Game, etc.). The variable changed is that of identification Experimenters weaken or abolish the condition of anonymity under which most games in the laboratory are conducted. Anonymity used to be an experimental standard, because identification can introduce pre- and post-experimental interactions that are difficult to control. Moreover, identification can introduce psychological effects (pride, shame, etc.) that override the treatment effect under study. Levitt and List (2007: 161) state that not being anonymous (toward the experimenter, for example). The argument is that individuals change their normal to more pro-social behavior once experimenters are watching. However, Bartmettler et al. (2012) state that there is only a minor pro-social effect that is not significant for the most commonly played games used in their experiment (Dictator Game, Ultimatum Game and Trust Game). Anonymity as a standard of experimentation has been explicitly questioned in the past (Andreoni and Petri 2004, Jentzsch 2012). If personal privacy is the object of scrutiny, the standard needs to be relaxed, otherwise the research cannot be conducted.[31]

These outcomes are often at odds with economic theory, sometimes refuting theoretical predictions. Factors other than money play a role in preferences, an observation that led to an active area of research on social preferences concerning fairness motives, inequity aversion, social reputation or type-based reciprocity.

Take the example of the Dictator Game. In this game, participants are paired, with one is acting as Dictator. He/she obtains a specific amount of money and can allocate a freely chosen share to the paired partner. The rest is kept by the Dictator. The most rational action in terms of utility maximization (numéraire: money) is to allocate zero to the partner. While the game is typically played in anonymity, the percentage of those allocating sums greater than zero significantly rises with decline of anonymity (Bohnet ant Frey 1997, Charness and Gneezy 2008). Assume an example where a Dictator is given 100 Euro and then allocates 9 Euros under conditions of anonymity. His monetary welfare is then 91 Euro. Now consider the same situation with identification of the other party with whom the Dictator deals. In this case a Dictator would allocate 25 Euros and reserve 75 Euros for himself. The reduction in welfare due to pro-social interaction based upon the identification would be 16 Euros for the Dictator.

Surveillance also makes a difference. Showing a pair of eyes on the computer screen is enough to significantly influence behavior. It introduces the feeling of being watched. The original study has been conducted by Haley and Fessler (2005) but has been replicated by others (see Nettle et al. 2013). It can be shown that this surveillance effect impacts on the probability to donate in Dictator Games, with pro-social behavior increasing in these games.

In Public Good games, as well as other donation contexts, there is a significant impact on the likelihood of donating once donors are identified (Andreoni and Petrie 2004; Jenni and Lowenstein 1997). In such games, individuals can contribute to a public fund either under conditions of

[31] There are a number of works that look at the effect of disclosure of pictures as a means of identification such as Fershtman and Gneezy (2001); in labour markets; Andreoni and Petrie (2008) in a repeated public goods game. They are not subject of the discussion here.

anonymity or under conditions where their name and donation amount are disclosed. In List et al. (2004) it is shown that as anonymity declined, an increasing number of people opted to donate money. Important was the degree of anonymity between subjects-experimenter and the subjects-subjects anonymity. The first refers to an experimental procedure known as single-anonymous and the latter to double-anonymous procedure. However, Bartmettler et al. (2012) found the experimenter effect to be insignificant.

Based upon the existing insights it can be assumed that the impact of identification varies with the degree of identification provided. As more individual information (name, date of birth, picture, ID number, etc.) is provided, the economic impact should increase.

3.2.3.1 Privacy Experiments without Secure Identification

In the following, we discuss additional types of economic experiments that do not restrict themselves to the typical games played in the laboratory. In Huberman et al. (2005), a reverse second price auction is used to obtain the private value for weight and age information of participants. Note that the participants in that experiment ***remained anonymous***. The authors show that deviation from the group's mean (in age and weight) asymmetrically impacted the price demanded for the information. However, neither age nor weight are entirely private information, both can be derived approximately by looking at a person. Visual identification is possible in the lab, though. While this is a pure information transaction, other research uses the composite transaction set-up. For example, Beresford et al. (2010) use a hybrid field experiment to analyse the willingness to pay for privacy. Participants were given the choice of buying a DVD from one of two online stores. One store required more sensitive personal data than the other. In the test treatment, when the DVDs were one Euro cheaper at the privacy-invasive firm, virtually all buyers chose the cheaper store. The authors conclude from their research that individuals are not willing to pay one Euro for their privacy.

3.2.3.2 Personal Privacy Experiments with Secure Identification

A complementary type of experiment is conducted by securely identifying participants with some public document (such as a picture-bearing ID or a student ID) and of abolishing subject-experimenter anonymity and subject-subject anonymity for the purposes of the experiment. Identification and public revelation of identity then explicitly becomes part of the game and of the strategic considerations that individuals make.

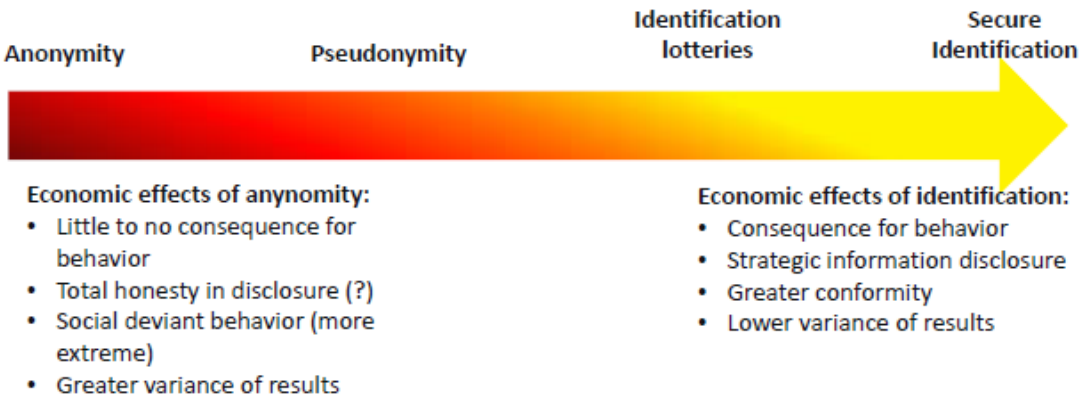
In Feri at al. (2016), individuals first take a logic test, after which they are privately informed on whether they are above or below the median score of the group in the laboratory. Next, they can sell this information when purchasing a real voucher. The price of the voucher can be discounted by disclosing the information to a firm. There is the risk of information leakage or a "privacy shock." Individuals selling their information to a firm whose data security is breached and who are unlucky enough to have exactly that period drawn by a random draw at the end of the experiment are revealed to the group with their name and their test result. In this research, it is shown that individuals act sensitively to the risk of leakage. Individuals with poorer test results, for example, are less likely to sell their information, giving rise to a strategic privacy behavior.

The same can be shown in a large-scale laboratory and field experiment conducted by the author together with co-authors (Jentzsch et al. 2012). Here, individuals can purchase cinema tickets from

two online stores, which are identical in the base treatment. The stimuli are the price as well as the amount information collected or the purposes for which the information is used by the store. The variation of the stimuli (i.e. just one stimulus from one treatment to the next) shows that while a privacy-invasive firm can undercut its competitor, the more privacy-friendly firm, there is a specific percentage of buyers who stay loyal to the privacy-friendly firm. Note that in this experiment, individuals are securely identified by checking their ID cards.

Due to space considerations, the hypothetical research and the survey-based experiments are not discussed herein. The interested reader is referred to **Table 4** for additional work in this area. In general, we can draw the following conclusions from the experiments reviewed (not all of them have been discussed here, though). A variance of the degree of anonymity and thus identification significantly impacts on economic outcomes (see **Figure 6**). Individuals tend to shed more egoistic behavior in favor of more pro-social behavior once privacy is diminished.

Figure 6 Identification and its Economic Impact



Source: The author.

The differences in disclosure behavior, depending upon secure identification, can be explained by the following example. Imagine the use of an Internet app for the calculation of individual net worth (based upon financial assets & earnings). These apps typically guarantee anonymity. [32] Now imagine the same service is provided, but the user is now securely identified with his/her legal identity. Would these apps be used and if so would individuals not have an incentive to "hide" information?

[32] Examples are: http://cgi.money.cnn.com/tools/networth/networth.html and http://www.tdcanadatrust.com/tools/planning/input_en.jsp

Table 4 Overview of the Research Field of Privacy Economics

Line of Research	Type	Explanation	Authors	Identification mechanism	ID verification
Empirical works (experiments and surveys)					
Classical experiments modified	IT	Traditional experiments are modified by introducing identification in Dictator Games, Ultimatum Game and other standard games. These experiments are incentivized with money.	Bohnet and Frey (1999), Charness and Gneezy (2008), Haley and Fessler (2005) Hoffman et al. (1996), Jenni and Loewenstein (1997)	In some works: name, in some pictures	None
Decision experiments *without* secure identity verification (SIV)	GT+IT	These are incentivized decision experiments that involve the purchase of a good together with an information transaction to be conducted by the subject	Beresford et al. (2012), Gideon et al. (2006), Huberman et al. (2005), Tsai et al (2011)	None BKP (2012): name	None
Decision experiments with SIV	GT+IT	These are incentivized decision experiments that involve the purchase of a good together with an information transaction to be conducted by the subject	Feri et al. (2016) Jentzsch et al. (2012)	Name, test result, DOB, mobile phone number	Yes, 100% checked
Auctions without SIV	IT	In these experiments, subjects use an auction mechanism to set the price for their personal data	Danezis et al. (2005), Huberman et al. (2005)	Anonymous, IMAI and location	n/a
Auctions with SIV	IT	In these experiments, subjects use an auction mechanism to set the price for their personal data	Feri et al. (2016), Jentzsch (2014)	Name, test result	Yes, 100% checked
Hypothetical scenarios					
Hypothetical scenarios	IT	Subjects are confronted with hypothetical scenarios of website policies, job search or insurance seeking	Andrade et al. (2002), Baumer et al. (2005), Egelman et al. (2013), Norberg et al. (2007)	None	None
Field experiments (including survey-based experiments)					
Field experiments (composite transactions)	GT+IT	In these experiments, subjects are not aware that they are participating in an experiment as they purchase a good on the website	Jentzsch et al. (2012)	Name, DOB and mobile no.	None
Field experiments (IT)	IT	In these experiments, subjects are not aware that they participate in an experiment as they answer a survey on a website	Hui et al. (2007), Rifon et al. (2005)	None	None
Other research (including methodological research)					
Data breach notifications and firm reputation	N/a	These works concentrate on the impact of announced data breaches on the stock prices of companies	Cavusoglu et al. (2004); Campbell et al. (2003); Muntermann and Roßnagel (2009)	N/a	N/a
Privacy metrics	N/a	In these works, different quantitative measures for privacy are proposed	Schulte-Melling (2014)	N/a	N/a
Privacy preference measurement	N/a	These are surveys that instrument the privacy concern by asking questions about attitudes, behaviors and perceptions.	Buchanan et al. (2006), Malhotra et al. (2004), Smith et al. (1996), Stewart et al. (2002)	None	None

Notes: IT denotes information transaction, GT denotes goods transaction, n/a denotes not applicable. Source: The author.

3.2.4 DATA BREACH NOTIFICATIONS AND FIRM REPUTATION

One of the central questions in the economics of privacy is how to improve incentive schemes in a market-conforming manner in order to achieve greater security of personal data. One suggestion is to make data breach notifications mandatory for firms. This is the focus of the literature presented below. In the EuroBarometer Survey EBS 359, an EU-27 average of 2 percent of Europeans was affected either by a data breach or by identity theft (statistic refers to 2011). In United Kingdom and Sweden even 5 percent of respondents were affected.

The point of departure for most works in this field is Eugene Fama's Efficient Market Hypothesis. According to this hypothesis, investors change their beliefs about future cash flow of firms once new information arrives. Therefore, stock market quotes always incorporate all publicly available information. Now imagine when a firm suffers a security breach. Once announced, the news alters investor expectations and should, therefore, be reflected in the stock price.[33] Data breaches can lead to increased marketing costs, litigation by affected parties, and forgone business for firms due to server downtime and reputational damage. The latter could potentially result in customer switching to competitors. Thus, data breaches should have a negative impact on the future cash flow of a firm.

One method to analyze whether data breaches have an effect on company reputation is the event study. Different researchers (listed in **Table 5**) use this methodology in order to extract insights on whether data breach notifications (to the market) have a negatively impact firm reputation.

The methodology works approximately as follows: As the stock returns are taken as indicator for company reputation, all companies, listed on the stock exchange, that were affected by data breaches are selected. Next, those affected by other confounding factors, such as stock splits or earnings announcements in the period of interest, are excluded. The remaining companies make up the research sample. A regression model is then estimated with returns as dependent variable and some stock index or basket of comparable firms as explanatories. The data for this estimation derives from a normal period. Then the expected returns are estimated for the event window (a selected timeframe around the occurrence of the event). Finally, the abnormal returns are calculated by subtracting the expected returns from the realized returns. This is done for all companies in the sample and the cumulative abnormal returns must be statistically different from zero, in order to claim that there was an effect of the data breach announcement on company reputation.

[33] Information on data breaches are collected by databases such as http://datalossdb.org/ and http://www.projekt-datenschutz.de/datenschutzvorfaelle.

Table 5 Overview of Data Breach Research (Event Studies)

Authors	Subject	Result	Sample	Study period	Match for CAR
Cavusoglu et al. (2004)	Security breaches of all types, 1996-2001	Loss of on average 2.1 percent of market value for breached firm **negative ST impact**	66 security breach announcements in U.S. traded firms, Internet and conventional firms	Short term: 2-day window	Market index (NASDAQ)
Kannan et al. 2007)	Breach effect on financial performance of publicly traded firms, effects of different types of breaches 1997 - 2003	Marginal decrease in market valuation (in comparison to control firms), Removal of 9/11 effect (firms hit in 6 months afterwards are taken out: overreaction), no effects of breaches **no impact**	72 breach events at publicly trade companies	Short term: 3-day window Long term: 8- to 30-day window	Similar firms as controls; but also market index
Malhotra and Malhotra (2011)	Data breaches (only customer data) effects on market valuation, 2000-2007	Data breaches lead to sig. market value depreciation, short and long term, larger firms are more affected **negative ST, negative LT impact**	93 publicly traded firms in U.S. , diverse industries	Short term: 1-day window Long term: 2-day window to 30-day window	Market index (NASDAQ)
Sinanaj and Munter-mann (2013)	IT security event (loss or stolen internal data) on firm reputation, 2004-2007	Public data breaches have negative impact on firm value, persistence of up to 5 days **negative ST impact**	72 events in financial and other industries in US, Europe, Asia	Long term: 5-day window	Market index (S&P500, etc.)

Source: The author. ST denotes short-term; LT denotes long-term. CAR denotes cumulative abnormal returns.

While the studies differ on the firms and types of data breaches surveyed, as well as the time periods covered, there seems to be quasi-agreement on the results. Data breach announcements noticeably impact the firm's reputation (measured in form of its valuation), but they do so only for a short time period. The negative impact seems to evaporate after only a few days (typically in the range of 2-5 days).

Policymakers looking for a lasting impact on a firm reputation, at least as reflected by stock prices, will be disappointed in this respect. If investors do not "punish" negligent security measures maybe consumers do? The hope is that consumers react in a way that induces market discipline for firms with respect to their security practices. After all, data breaches could lead to a decrease in trust, to annoyance, and, ultimately, switching activities. The problem is that in this area, there is not a lot existing research to learn from and there is first anecdotal evidence that consumers do not switch in masses after a data breach has occurred.

There are reports by the Ponemon Institute that – based upon estimates of the management – about 2-4 percent of clients end their contractual relationship after a data breach.[34] Abnormal churn rates were calculated for this; i.e. the loss of customers who directly received a breach notification. The study found that the industries with the highest churn rate were pharmaceuticals, communications and healthcare (all at 6 percent), followed by financial services and services (both at 5 percent). Note that at this stage there is no rigorous experimental insight on switching.

Somewhat surprising are the results from a study on the effects of breach notification on online consumers in the laboratory (Feri et al. 2016). Here, consumers conducted a logical test similar to an intelligence test, and were privately informed about the test result (>/<median of the group). They could buy one voucher per period in the two-period game. They were given the possibility to reduce the price of the voucher by disclosing their name and test results. Moreover, there was the risk of having the data disclosed to the other lab participants. In the baseline treatment, there was no notification about data breaches between the periods, whereas in the notification treatment, individuals were informed whether their privacy was compromised.

The results show that negative information (i.e. being below median of the group) was less likely to be disclosed (thus, there is a preference for privacy). While data breach notification should not make a difference in disclosure behavior, because probabilities of breach per period are independent, individuals who are informed that a breach had occurred tended to continue to disclose the data in the next period. One possible explanation is the so-called bomb crater effect, where individuals do not think they will be hit again by a privacy breach has taken place.

All in all, there is insufficient evidence on the impact of data breaches on firms and consumers. While there are a number of studies on the impact for firms, little is known about consumer switching behavior. This should be tackled by future research in order to gain insights into whether or not making breach notifications mandatory is a useful instrument for increasing market discipline.

3.3 Privacy Preference Measurement

Finally, there are a number of works that measure of privacy preferences. The basic problem in question-based research is that the very act of asking questions about privacy could prime individual and increase concern. Some measure concerns using Likert-scaled answers. Likert-scaled answers are the replies of survey respondents to questions on privacy, measured by a scale of 1 to 7, for example.

The authors typically propose a series of questions (Buchanan et al. 2006; Malhotra et al. 2004; Smith et al. 1996, Steward and Segars et al. 2002). This approach in itself bears problems. Through factor analysis, different dimensions of privacy concerns are derived. However, these authors do not test whether the stated preferences associate with real behavior, let alone predict it. Only one work is discussed here as an example here; an overview of additional work is provided in **Table 6**. This is necessarily only a limited introduction to privacy preference measurement; a general overview is provided by Preibusch (2013).

[34] Ponemon Institute, http://www.ponemon.org/news-2/23.

Table 6 Measurement of Privacy Concerns

Authors	Year	Measurement	Approach
Malhotra et al. (2004)	**2004**	IUIPC: Multidimensional notion of Internet Users data Privacy Concerns (IUIPC)	The measurement instrument recognizes multiple aspects of data privacy: (i) attitudes toward the collection of personal data; (ii) control over personal data; and (ii) awareness of privacy practices of companies gathering personal data as being components of a second-order construct they label IUIPC. All of these aspects still lie within the domain of informational privacy.
Buchanan et al. (2006)	**2006**	3 Internet-admin scales measuring privacy concern	In the first study there were several people who completed an 82-item questionnaire from which three scales were derived. Then the correlations between the scores on the current scales and two established measures of privacy concern were examined.
Smith et al. (1996)	**1996**	Concern for Information Privacy Scale	15-item instrument to measure individuals' concern regarding organizational practices. It identified four factors—collection, errors, secondary use, and unauthorized access to information as dimensions of an individual's concern for privacy.
Stewart et al. (2002)	**2002**	Re-evaluation of: Concern for Information Privacy Scale	Study examines the factor structure of the concern for information privacy (CFIP) instrument posited by Smith et al. (1996). The results suggest that each dimension of CFIP is reliable and distinct. However, CFIP may be more parsimoniously represented as a higher-order factor structure rather than a correlated set of first-order factors.

Source: The author.

An early work is Smith et al. (1996), who developed the Concern for Information Privacy Index. This index is a 15-item instrument that measures the stated concerns of individuals regarding organizational practices with respect to personal data. The instrument asks a number of questions, with individuals responding on a 5-point Likert scale (how strongly they agree with a statement). It identifies 4 factors as most important: collection, error, secondary use, and unauthorized access; which the authors term the 4 dimensions of privacy concern. The instrument was used in Jentzsch et al. (2012). The authors tested its relationship with the actions of same individuals in the laboratory with little success (i.e. no or only weak correlation). A very simple classification is proposed by Westin quoted in Kumaraguru and Cranor (2005), who categorizes consumers into privacy fundamentalists, pragmatists, and the unconcerned. However, this classification proved to be not predictive for any choices of individuals regarding their data in a purchase transaction (Feri et al. 2016).

Other studies use action-based instruments for concerns, such as the number of personal data items disclosed (John et al. 2010), or the reply to specific questions in online marketing surveys (Goldfarb and Tucker 2012). In general much more research needs to be invested into robust preference expression and identification.

3.4 Privacy Metrics

Recent advances in research challenge the notion that measures related to privacy are not quantifiable. This field can be broadly termed "privacy metrics". It is to some extent unrelated to the aforementioned works on privacy economics. It is included here as a methodological advancement. Privacy metrics are related to two main areas:

- Key performance indicators as used in firms or by policy makers; and
- Theoretical algorithms that are related to the sensitivity of data in a given dataset.[35]

[35] The sensitivity is the risk of being revealed once drawn from a dataset.

In what follows, I discuss **privacy metrics as key performance indicators** in a "return on investment" context. Such metrics range from a number of data security incidences to the number of privacy impact assessments conducted in a company. The main goal of this approach is to make privacy (aspects) in firms measurable and comparable. Such an approach, which is arguable of course, would enable inter-temporal trend comparisons, and might enable justification of Data Protection Officer's budgets in firms.

Privacy Risk Exposure: The privacy risk exposure is typically an outcome of a Privacy Impact Assessment. As a single variable it can probably be best described as potential loss resulting from the compromising of personal data held by a firm. Important is the probability with which a data breach could occur. The input to such a calculation is often not more than informed guessing; therefore the indicator is more qualitative than quantitative.

Return on Privacy Investment: For a suggested privacy metric, the return constitutes the avoided potential losses through data breaches, *Annual Loss Expectancy (ALE)*, where *ALE = single loss expectancy (SLE) * Annual Rate of Occurrence (ARO)*.[36] SLE describes potential losses, ARO the frequencies of such losses. *Red*, in the formula below, denotes the reduction in frequencies of breaches occurring (say from 10 cases 8 can be avoided, 0.8). Finally, *cost of measure* indicates the costs for the implementation of the protective measure. Thus,

$$ROPI = \frac{(ARO*SLE)Red - Cost\ measure}{Cost\ measure}.$$

If the result is greater than 1, the protective measure can be regarded as cost efficient by the investor. Again, the inputs into this formula are rather indicative and often subject to informed guesswork. Any output inherently reflects this problem. Therefore the outcome of this calculation should be accompanied by a confidence estimate regarding the quality of the outcome.

3.5 Other Key Privacy Risk Indicators

There are also a variety of other privacy indicators that are currently in use. Note that at this stage, a comprehensive overview of risk indicators cannot be given, as this exceeds the purpose of the general literature overview. Key privacy risk indicators are indicators such as sensitivity of personal data, the volume, complexity (number of partners involved in processing and exchange), as well as the costs of breaches of data security as well as international interaction and contracting, i.e., if more and more diverse partners are involved in the data processing, the risk increases. Costs of data breaches may also be used as key performance indicators.

[36] The following is based upon a presentation given by Jyn Schultze-Melling at the 15. Datenschutzkongress in Berlin.

Table 6 Costs of Data Breaches

Cost category	Cost components
Direct expenses	Digital forensics Customer support Marketing measures Consumer notification Litigation and legal fines
Indirect expenses	Customer loss due to switching (so-called turnover) Lower customer acquisition rate in future

Source: The author.

While the use of metrics might enable comparisons, a number of tedious problems remain. The first is that it is often not defined what a data breach is; after all in many European countries, data breach notifications are not mandatory (ENISA 2011). In the proposed draft of the Data Protection Directive, a personal data breach is defined as, "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."[37] If data breach notifications are made mandatory, there could be an incentive to invest in greater security. But this discipline could more stem from potential punishment delivered by authorities as opposed to that delivered by the market (see discussion above on the impact on market valuations of companies). A second important problem is that we do not know how to exactly estimate the loss stemming from such breaches. Here a recommendation is to further develop the techniques that exist to compile information on the aspects mentioned in Table 6.

In general, the estimates with respect to data breach costs vary widely, where some estimate 3.50 USD/record (Netdiligence's estimate in 2012), others suggest up to 200.00 USD/record (Ponemon Institute's estimate for 2012).

The interested reader is referred to the **Overview Table** (**in the Appendix**), which provides an overview of the industry reports. The main problem associated with these reports is that the issuing source often has an incentive to over-estimate the threat, if it is a commercial security products provider, or to underestimate it, if it is a public authority. The widely varying estimates are also due to the very different methodologies that are used in these reports. Examples of methodologies include:

- Surveys of firms and organizations affected by cybercrime/data breaches;
- Surveys of adults affected by cybercrime/data breaches;
- Malware tracked by the respective security provider;
- Attacks neutralized by the software of the security provider; and
- Complaints databases.

[37] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, source: http://eur-lex.europa.eu/legal-content/en/ALL/;ELX_SESSIONID=xfJ1Th2JxC9M5phWxNpQTGGt1hRkfxpGln2TyNBJM7yBbsHQFpSh!-1392697299?uri=CELEX:52012PC0010.

All in all, the policymakers ought to opt for a standardization of the reporting of data breaches not just across sectors and industries, but also across Europe. This is the intention of the ePrivacy Directive and there are currently plans to reform the current reporting structure with the new Data Protection Directive framework. It is stated there that the data controller should, as soon as he becomes aware that such a breach has occurred, notify the competent national authority of the breach. The individuals whose personal data or privacy could be adversely affected by the breach should be notified without undue delay in order to allow them to take the necessary precautions.

3.6 The Economics of Privacy Seals

Another nascent area of research in the economics of privacy is the impact of privacy seals and/or certificates on consumer decisions. Privacy and security seals are intended to certify the conformity of products and services with data protection laws, thus helping consumers to choose more privacy-friendly products. Technical security seals on the other hand, certify the compliance with specific technical standards, including ISO standards. Some examples are the European Privacy Seal, UDL Privacy Seal, D21 Initiative (Trusted Shops Guarantee), the TÜV SÜD Safe Shopping Seal, and the seal of the Euro Commerce Institute (EHI Retail Institute). The seals differ in their analysis of compliance, as well as certification costs, ranging from free to 15,000 Euros or more, depending on the business model chosen by the provider of the certification.

A seal is a visible sign of compliance. Seals can be granted by public or private institutions. If they are granted by the latter, the business model of the certifying institution includes payment by the applicant. Seals can be an important market-conforming measure to increase consumer protection and potentially also consumer trust. In the European Commission's published proposal, it is recommended, in Article 39, that the Commission and the Member States support the development of data protection certification mechanisms, labels and similar IT trust marks. There is, at the moment, little robust empirical research on privacy seals, their impact on company security, as well as on the behaviour of consumers. Policy and research needs to invest more in order to better understand how seals, company reputation, and consumer action interact with one another.

Companies will only invest in a seal if a significant number of consumers, who value this product/service trait, alter their decision based on the presence of the seal. As an additional product feature that becomes visible to consumers, certificates can be used to increase prices, as the product is differentiated in one more dimension (not only in prices and in technical characteristics).

However, with an increasing number of competing seals, it becomes easier for a firm to obtain one. Ultimately seals could become meaningless to consumers. A variety of seals provided by competing institutions can reduce comparability. Consumers would have to know the different seal-granting mechanisms in order to be able to compare them. Consequently, trust in a seal is largely derived heuristically from the reputation of the certifying institution (e.g. Stiftung Warentest in Germany). It is striking that in this important area on the economics of privacy, there are only a very few empirical studies and even fewer experimental ones. Moreover, the author could not identify any natural experiments in this area.

There are a number of survey-based experiments on this subject, but their informational content, in terms of explaining real impact on consumer action, is low. One problem is that, in order to make significant claims, there needs to be a large number of observations, which is difficult to achieve.

Moreover, if the experiment is not implemented in a clean and proper way, it is unclear whether a causal effect of the stimuli displayed is actually measured.[38] In addition, in real purchase transactions money is at stake, which is not the case in hypothetical scenarios or survey-based experiments.

Table 9 Privacy Seals: Experimental Studies (Chronological Order)

Authors	Typ transaction / experiment / subjects	Results
Rifon et al. (2005)	- Incentivized information transaction - Invitation to a website with hypothetical purchasing situation - Questions about the perception of the subjects, 210 responses from subjects (undergraduate students)	Privacy seals increase the expectation that a company is transparent with respect to handling of the data - Privacy seals induce trust - Privacy seals have no effect on the intention to disclose personal information (real actions were not tested)
Gideon et al. (2006)	- Incentivized purchase transaction - Internet shopping situation in the laboratory - 24 subjects (students)	- Implementation of privacy promise as visual (as in Egelman et al. 2010) - If privacy policies are presented as a visual, they influence the selection of the provider in sensitive purchases
Hui et al. (2007)	- Incentivized information transaction - Invitation to the website with a filled out survey, participation of 109 subjects (students)	- Privacy promise increases information disclosure - Privacy seals do not increase information disclosure
Egelman et al. (2010)	- Incentivized purchase transaction - Use of Internet search engine in the laboratory with privacy seals for purchase transactions - 89 subjects (students)	- Implementation of privacy promise as visual - If privacy policies are presented as simplified visual, they influence the selection of the provider in sensitive purchases

Source: The author.

Table 9 gives an overview of the behavioural experiments that the author identified. For example, in Hui et al. (2007) the authors worked with a local company, which hosted the experiment on its website under its real domain name. Participants were not informed of the experiment and could fill out a survey sheet of the company in exchange for payment. The experimenters varied the situations under which the subjects filled-in the questionnaire. A major finding of this study is that the existence of a privacy statement enticed more participants to provide personal data. However, the existence of a privacy seal did not. A monetary incentive had a positive impact on the disclosure of information, while increased demands for information had a negative impact. According to these findings, it makes a difference for the competitive strategy of a company whether it is investing in a privacy seal or whether it displays a privacy policy.

[38] For example, if the effect of the presence of a privacy seal is tested and the seal is displayed as traffic sign showing different colors, it is unclear if test persons react to the colors or the presence of the seal.

In Egelman et al. (2010) a purchase experiment was conducted, where participants could first buy a pack of batteries and then a sex toy. The providers differed in their protection of personal data afforded to the buyers. The result of this study is that displaying of data protection in the form of a visual cue that causes buyers to include data protection in their decisions. They then tend to buy from online retailers who guarantee a higher protection of privacy, especially if they are purchasing a sensitive good. Note that the number of the participants was rather low in this experiment (89 participants) and multivariate empirical analysis is not possible with the data.

Relation with PACS development and adoption:

If no robust models of certification are developed which can work as a competitive advantage for the certified firms, there will be no viable market in the long-run. Companies will not have an incentive to invest in a privacy seal and, consequently, no products or services in the area will be developed. The European Union would lose the opportunity of setting international standards in this area, as security products made in the European Union could potentially gain attraction in the international markets.

Area of future work / extraction of questions:

- Policy makers should support evidence-based insights: instead of relying on surveys, they should support laboratory and natural experiments;
- Much more robust research needs to be conducted in this area; and
- Minimum standards are necessary for trusted privacy seals. A regulatory authority may improve the information content, as well as the comparability, of seals by providing minimum quality requirements for certification.

3.7 MONETIZATION OF PRIVACY

The term "monetization of privacy" describes the commodification and sale of personal data and the decline of personal privacy that comes with it. Before we discuss the economic value of personal data, one ought to start with the fundamental question of the incentivization of personal data disclosure. **Economic incentivization introduces a monetary or other type of cash-value reward into an exchange.**

Incentives activate self-interested behaviour and may undermine pre-existing intrinsic motivation (Grant 2012). While Grant refers to other kinds of examples, her insights are enlightening when thinking about the treatment of human behaviour as if everyone has a price, including a price for privacy.[39] A number of difficult ethical problems arise with incentivization. For example, it can be argued that offering a big amount of money to a poor person is coercive and has little to do with free choice. Such moral and ethical dilemmas will also surface when considering the incentivization of

[39] See Koehn (2012).

personal data disclosure. It may crowd-out other types of social exchange of personal data, other motivations of disclosure, and lead to pre-selection effects **on both sides of the market**.

- Incentivized disclosure will be most attractive to those most in need of the incentive. For these individuals the incentive provides the greatest motivation.

- The information disclosed will likely go to the highest paying requester. This will likely affect the current information flows in the market and lead to information concentration in market-dominating firms, strengthening the ongoing concentration tendencies in the market.

If the disclosure of personal and private information (thus, a reduction in privacy) is incentivized, it may crowd out other types of exchanges as well as non-monetary motives. Moreover, it might lead to an actual reduction of privacy, instead of increasing it; assuming privacy is the policy goal. A more extreme point of view is that it might leave a society where poorer segments of the population shed privacy for money, while the well-off segments retain their privacy or only shed it if the price is comparatively high. Policymakers should better think through what economic incentivization really means in the field of personal data and what developments it will spark for society.

3.8 Economic Value of Personal Data

The economic value of personal information is one of the most controversial areas in the academic literature, where the opinions vary from determining exact prices for profiles to no prices are feasible at all. A number of international institutions are now addressing the issue. The World Economic Forum (WEF) termed personal data as a "new asset class" (World Economic Forum 2011). It states that companies, such as Facebook, Google, and Twitter, are showing the importance of personal data collection, aggregation, and monetisation. In the WEF report, the stakeholders and value chains, with respect to personal data, are identified (as displayed in **Figure 7**).

The OECD published a report on exploring the economics of personal data, which is presenting different methods for estimating the value of personal data (OECD 2013). These methods include:

(i) Estimation methods derived from the financial figures of a company divided by the number of data records held by that company;

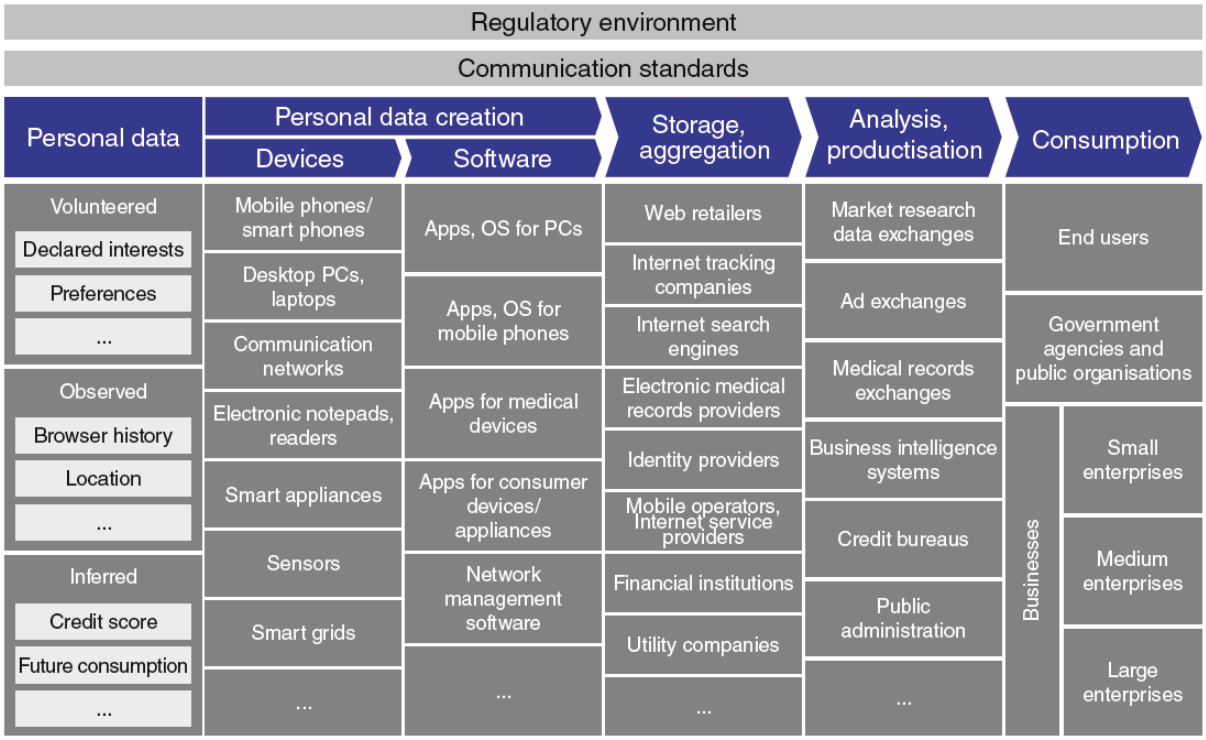
(ii) Market prices of personal data records;

(iii) Illegal or black market prices of data records; and

(iv) Surveys and economic experiments.

In the following, these methods will be summarized and critically discussed. In a second step, it is elaborated on the mechanism design. This stream of work can be considered to be basic research, a nascent area that needs to be better developed in the future.

Figure 7 Value Chains in Personal Data Production and Usage



Source: Bain & Company

3.8.1 VALUATION OF PERSONAL DATA

In order to obtain a rough idea on the pricing of personal data, the OECD (2013) has analyzed several indicators that are derived from real markets, not experimental ones. Ideally, the researcher would like to obtain an unbiased estimate of the valuation of personal data. But a number of factors impair this possibility. Researchers can at this stage only strive for obtaining an *unbiased as possible estimate* of the valuation of personal data, because realistically it might be impossible to obtain an *unbiased estimate*.

Indicators based on Market Valuation of Personal Data

Table 7 shows that none of the presented measures of valuation is ideal. The indicators (1)-(4) are noisy because market players typically also price-in other factors that are not directly related to the intrinsic value of the personal data held by a company. The least noisy one among these is indicator (2), because it reflects market supply and demand conditions. However, as discussed in the introduction to this chapter, personal data's peculiar traits and externalities can lead to ***biased market prices.***

Another important aspect is that in measures (1)-(4), the data subject is not directly involved in the pricing of the information, as third parties (Internet companies, data brokers) are trading the information. This means that the valuation of the data by the subject is not explicitly reflected in the pricing on the downstream market. Therefore:

- Market-based valuations are not guaranteed to give an unbiased estimated of the "true value" of personal data due to market biases related to problems of asymmetric information and information externalities;
- The incentivization of personal data disclosure can lead to pre-selection effects, with only those disclosing who have the greatest incentive to do so;
- The market structures and pricing models can be very different from each other. For instance, compare the market for social networks with that for credit reporting agencies; and
- The data subject is frequently not involved in the information trade.

There are works on the differences of the Willingness-to-accept (WTA) versus Willingness-to-Pay (WTP) for privacy (Acquisti et al. 2013), which are only briefly mentioned here. In essence, one of the conclusions of the authors is that the maximum price persons are willing to pay for privacy diverges from the minimum price persons would accept in order to sell their data. The problem is that the original behavioural argument, the so-called "endowment effect"[40] is challenged in economics. In fact, the WTA-WTP gap disappears, once it is controlled for the understanding the mechanism by the experiment participants and once it is controlled for anonymity by the experimenter (Plott and Zeiler 2005, 2007, 2011).

Indicators based on individual valuations or experimental markets

Researchers have implemented different techniques regarding extraction of revealed valuations. For example, in experiments, take-it-or-leave-it offers have been implemented in forms of offering discounts on goods sold in the lab to subjects. The participants either accept or reject the offer, which is a binary decision (Jentzsch et al. 2012). This setup logically leads to either high or low valuations of privacy. Another method for price-setting is the auction, where the reverse Vickrey auction is used (Huberman et al. 2005, Jentzsch 2014). However, there are indications that this mechanism is not well-suited as there is no dominant strategy for players in the presence of privacy costs. Moreover, some experiments offer personalization of the product in exchange for personal data, which can save on time costs once individuals return to the same firm.

Box 6. Online Data Valuation Tools:

There are a number of online tool that offer the possibility to estimate the value of personal data. One example if the Financial Times personal data value app. Other apps in this area is the Swipe Toolkit or PrivacyFix.

However, experimental elicitation of valuations might be neither internally nor externally valid. Internal validity demands that a causal inference drawn from an experiment is justified given the experimental design and conduct. External validity allows the generalization of the results to other persons and/or situations. Pre-selection effects are particularly strong in research that uses social network data (see also Ruths and Pfeffer 2014).

[40] The gap between a subject's willingness to pay (WTP) for an item versus the willingness to accept (WTA) dispossession of the same item.

Table 7 Summary of Measures of Value of Personal Data with Modifications

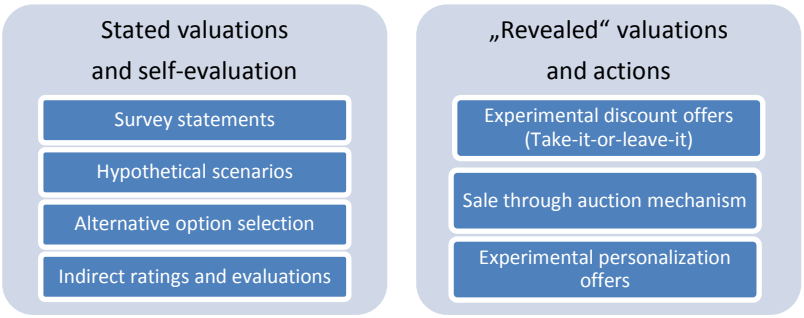
Indicator	Description	Benefits	Potential Drawbacks
Indicators based on market valuation			
(1) Financial results per data record	Aggregated market cap (revenues, or net income) of a company divided by the total number of personal data records held by this company.	- Relatively easy to identify. - Reflects perceived value added generated through personal data.	- Inaccurate as numerous other components impact market capitalization / revenues / income of a company. - Accuracy of this approach depends on what portion of profit is directly tied to personal data sale.
(2) Market prices for data	Price per personal data entry offered on the market by data brokers.	- Relatively easy to identify; - Reflects market value of a given data set.	This measure neglects the context in which the data is sold, which has a large influence on the demand (and price) for data.
(3) Cost of a data breach	Economic cost of a data breach (for firms and individuals) per data entry.	Reflects a market value and some of the risk that companies must protect against.	Captures market costs of damage caused by data breach rather than value of data themselves. Does not include the costs of damage to a firm's reputation.
(4) Data prices in illegal markets	Estimation of prices of personal data in illegal markets.	Reflects market value of a specific data entries or data sets.	Only applies to data that is re-used illegally. Because criminals must balance the risk of detection and punishment, the value of the personal data on this market reflects this trade-off.
Indicators based on individual valuations or experimental markets			
(5) Surveys and economic experiments	Valuation of personal data in monetary terms are reported / revealed by individuals in surveys / economic experiments.	- Captures the pure economic value of personal data from an individual perspective. - Depending on setup, results can lack internal and external validity.	Hypothetical valuations are not verified by the market. Valuation of data is highly sensitive to context (the way questions are phrased) and this could significantly alter the responses
(6) Individual willingness to pay to protect data.	Amounts that individuals are ready to spend to protect their personal data.	- Either captures the economic value of privacy or appreciation of technical security by individual.	Captures individually perceived aggregate costs of damage caused by data breach, rather than value of data themselves.

Source: OECD. Note that this Table has been modified by the author. These modifications might not reflect the opinions of the original authors.

In addition, most experimental studies analyzed by the author do not implement an **incentive-compatible mechanism**. Under such a mechanism a player maximizes his/her economic payoff by revealing truthful information (in terms of valuations or personal data disclosed). That is, in general, in many studies it is not clear what the ***quality* of the information** disclosed by study participants is and whether they have possibilities to disclose manipulated information. It might be that for some types of players (these with high privacy concerns) disclosing falsified or manipulated information is a dominant strategy, as the payoff is maximized and privacy is cushioned by disclosing manipulated information.

With respect to indicators (5)-(6) of **Table 7,** we can expect that these more closely reflect the individuals' intrinsic value of personal data. However, **hypothetical statements** are not reliable. This is not to say that statements are not informative, but their informativeness needs to be tested. For example, in the area of risk perceptions measures, there is ample discussion whether stated or action-based measures are adequate (see Dohmen et al. (2011) for a discussion on risk perception measures).

Figure 8 Mechanisms for Elicitation of Valuations of Personal Data



Source: The author.

At the most basic level, two types of elicitation methods can be differentiated; see **Figure 8**. The first is based upon stated valuations as well as self-evaluations of individuals and/or expert evaluation. For example, in surveys individuals are asked about their estimate of the value of their personal profile. Moreover, some use expert interviews to derive the value of personal data held by a company (Compass Intelligence 2013: 9). Such methods include hypothetical scenarios presented to individuals with alternative options from which they can select their most preferred one. Indirect questions and evaluations could be what respondents think others would pay for their personal data (Compass Intelligence 2013: 9).

Note that for the different elicitation mechanisms, it holds that individual valuations of personal data are likely to be *biased* for a number of reasons e.g. the simple reason of being in a laboratory, specific priming, and/or framing of questions. Hypothetical statements are often not associated with real valuations. Real valuations, on the other hand, seem to be largely context-dependent.

For example, much of the situational valuation or disclosure quantity obtained in experiments is subject to the framing of questions or to permission formats, such as opt-in versus opt-out (Johnson et al. 2002). Therefore:

- Experimental elicitations of valuations of personal data directly from data subjects do NOT guarantee unbiased estimates of the "true valuation," because the mechanisms implemented are not incentive-compatible;
- Mechanisms that are not incentive-compatible lead to biased estimates of the revealed valuation; and
- There is the need to develop elicitation mechanisms that are as unbiased as possible, to the best of our knowledge.

3.8.2 BUSINESS MODELS OF PERSONAL DATA INTERMEDIATION

Despite the aforementioned biases associated with the valuation of personal data, businesses have found a number of ways to circumvent or reduce these problems. That is, the players have developed different ways to entice consumers to disclose personal or semi-personal data, which evolved into very different business models. The most important ones are summarized in **Table 8** below. This can be instructive for the development of innovative PACs.

Identification or proxy identification – The first and foremost distinction regarding business models is whether individuals disclose personal data connected to proxy identifiers or their legal real and natural identity or they disclose nothing. Technical proxy identifiers include, for example, IP addresses, mobile phone IMEI information, numbered bank accounts and user names. To a certain extent they shield the "natural identity" of a person, although not perfectly. Legal identity includes real name, address, date of birth, as well as identifiers such as ID card numbers. This information allows individuals to be uniquely identified, at least with the power that a state would have to identify its citizens.

Table 8 Pricing of Personal Data: Business Models

Business model matrix	Identification of user		Monetary incentives		Non-monetary incentives	Third-party data sharing
Company name	ID Proxies	Legal ID	Earnings	Payments	Personalization	Revenue sharing
Acxiom	(X)				X	no
Bluekai	(X)					no
Equifax		X	X	X	X	no
Experian		X	X	X	X	no
Facebook	X				X	no
Foursquare	(X)				X	no
Google	X				X	no
Groupon		X				no
Handshake			X			yes
Reputation				X		no
TransUnion		X	X	X	X	no

Note: In credit reporting (Experian, TransUnion and Equifax), banks typically price in the price of a consumer report requested on the applicant. While a good risk could get lower prices, a high risk will get a mark-up for credit taken up. The net effect depends on the circumstances. (X) denotes that once these firms also collect ID numbers, such as SSN in the U.S., they would have the legal identification of data subjects.

Monetary or non-monetary incentive – The second important distinction when looking at business models is how individuals are incentivized to disclose personal data. Are they directly being offered a **monetary benefit** (e.g. the Handshake business model) or do they obtain reduced prices in form of discounts (e.g. Groupon business model)?[41] Do they need to *pay* in order to control more their information (e.g. Reputation.com, credit reporting)? The mechanisms at work here are quite

[41] From Neuroscience it can be learned, how consumers react to price discounts (Chen et al. 2012).

different to the mechanisms at work for social exchange, where non-monetary incentives play a role, at least in the primary transaction between data subject and service provider.

If data are disclosed for **some other benefit** such as personalized search engine, website or other service (e.g. Google, Twitter, Facebook), non-monetary incentives play a role in the exchange, such as reciprocity and fairness. Loyalty programs also fall into this category, as they enable a firm to collect a more detailed customer profile and to increase the switching costs of their customers by providing loyalty bonuses.

No Participation in Third-Party Sales and no Revenue-Sharing

It is noticeable that in *most known business models,* the data subject does not actively take part in the secondary transaction, where their data are commodified and monetized. These models hold for online advertisement (Google, Facebook) as well as credit reporting (Equifax, Experian, TransUnion) and direct marketing (Acxiom).

Participation in Third-Party Sales and/or Revenue Sharing

There seems to be an increasing number of start-ups that provide consumer-direct services, where consumers directly participate in the revenue sharing from third-party data sales. These companies are also called data vaults, data lockers or personal information management systems (PIMS). They offer consumers a supposedly safe place to store personal data (either by linking bank accounts or storing utility bills, telephone records, etc.). Some provide services, such as pre-filling of web-forms, or enable a more holistic view of one's finances (banking apps), while others provide a link to government services.

Some of the companies in this market segment closed after test runs or issuance of beta versions, for example Jini and Mydex.com. Other firms were purchased by large data providers (MyID.com is now Experian-owned). Examples of companies and apps that are still running include Handshake, Mint.com, Qiy digital me and personal.com.

Voluntary participation in these schemes will lead to a skewed distribution of participation, as it can be expected that technologically savvy and less concerned persons take advantage of these schemes. For the privacy-concerned it is yet another firm to which data is disclosed, which increases the risk of having personal data compromised. These persons might select themselves into anonymity product and services segments of the market.

3.8.3 MECHANISM DESIGN

The development of incentive-compatible mechanisms to extract truthful valuations of personal data, the most important area in the economics of privacy, is the probably most under-researched area at this stage. In the past, economists primarily focused on mechanisms that provide truthful valuations of indivisible private goods that are scarce. There are a number of established mechanisms that we know are incentive-compatible (Becker-deGroot Marschak, BDM, or second-price Vickrey auction, for example). Unfortunately, as stated in the introduction to this chapter, personal information is a different kind of good. It virtually does not fulfill some of the classic characteristics of tradable goods. And while incentive-compatibility is an important concept for

volunteered data, many data subjects are not aware about traffic data or statistical inferences that are based upon samples. In this case policymakers ought to strengthen choice by facilitating markets for anonymity products and services.

In **Table 9** a brief overview of the mechanisms used and the outcomes of personal data valuations is presented. Note that only experiments using money as numéraire are considered and not experiments using social exchange of personal data.

Table 9 Valuations of Personal Data

Authors	Transaction	Mechanism	Revealed valuation	Decision modality
Beresford et al. (2012) Jentzsch et al. (2012)	Purchase transaction	Take-it-or-leave-it	Amount of discount	Binary: accept/reject
Bohnet and Frey (1997) Charness and Gneezy (2008)	Allocation in Dictator Game	Allocation	Premium allocated considered anonymous decision	Discrete
Andreoni and Petri (2004) Jenni and Loewenstein (1997)	Allocation in Public Goods Game	Allocation	Premium allocated considered anonymous decision	Discrete
Huberman et al. (2005) Jentzsch (2014)	Reverse second-price auction	Ask price	Direct sale price	Participation in auction: binary Ask price: discrete

It is important to note that the framing of the decision – whether a binary (yes/no) or a discrete choice (counts)[42] – yield different distributions of personal data valuations by their subjects. There are also a number of theoretical works on the pricing of personal data and the privacy-personalization trade-off. Regarding the former, Aperjis and Huberman (2012) proposed paying individuals according to their privacy concern/risk attitude; as does Gkatzelis et al. (2012). In Roth (2012), pricing takes privacy costs into account. **A precondition for these mechanisms to work, however, is the identification of reliable and informative measures of privacy concern as well as of privacy costs.** As discussed in the section on privacy preference measurement, it is a complex task to measure privacy concerns and once mastered, it is still an open question whether they are predictive of an individual's actions. The privacy-personalization trade-off is subject to a study by as well as Chellappa and Shivendu (2010).

3.8.4 Differential Privacy

Differential privacy is the latest development in mechanism design. These works take into account that, "agents desire that not much of their information be revealed to any other agent via participation in (a) mechanism" (Kearns at al. 2014: 431). That is, the players have types that are payoff-relevant and they know that by participating in the mechanism their type could be revealed. A mechanism (or algorithm) is differentially private, if its output is insensitive to the change of a single input. As Chen et al. (2013) note, differential privacy is a property of the algorithm and there is a trade-off between privacy and the accuracy of statistics computed from the obtained data.

[42] Monetary amounts are often treated as continuous variables.

The authors explain that *incentivization* gives players influence over the outcome, but this influence automatically leads to privacy costs – by changing the outcome in one or the other direction (for example through participation or non-participation in a mechanism), it reveals something about a players type.

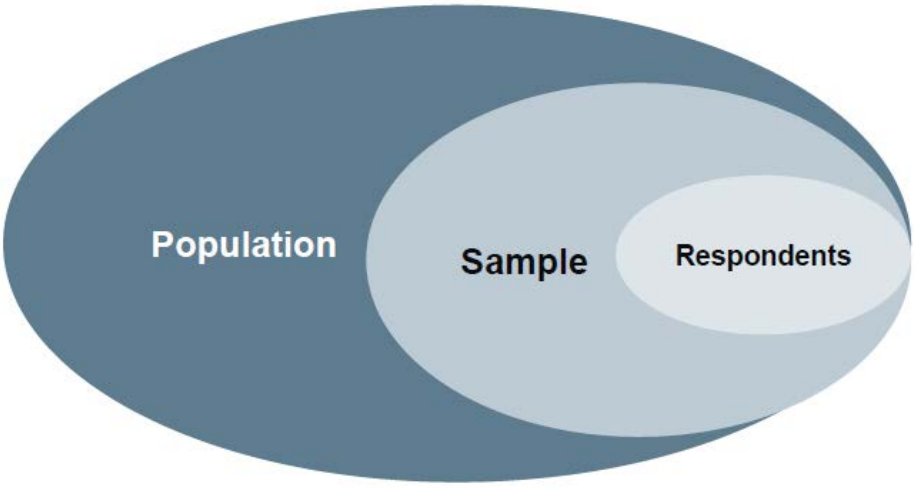
The question is whether a player can change the outcome of the mechanism by using a strategy of lying or manipulation of the released information. Players valuing their privacy will have an incentive to not report truthfully, as discussed above. Xiao (2013) shows that it is possible to design mechanisms that simultaneously result in truthfulness and differential privacy.

3.8.5 SKEWED DISTRIBUTIONS AND SKEWED RESULTS

The above discussion also links to the problem of skewed distributions, mentioned at several places in this document. These skewed distributions of participation in a database or mechanism arise for two reasons: (1) intrinsic privacy concerns; and (2) incentivization. Before personal data is collected, an individual needs to decide about their disclosure, which ideally reflects the **intrinsic privacy concern** of the individual. However, if the participation in a mechanism reveals sensitive information, individuals might decide to not participate in the first place, leaving a skewed distribution of participants in the mechanism. This can lead to sampling bias (see **Figure 9**).

The same issue emerges with participation in social networks. When research on privacy makes use of a dataset of social network participants, it must be made clear that this is a biased selection of largely privacy-insensitive individuals (for a critical discussion of research using social network data see Ruths and Pfeffer 2014). Consequently, the results are biased and not valid externally. Privacy-sensitive individuals will not participate in the network, but it is not only them. There might be a number of other psychological factors, such as an aversion to image cultivation that leads to non-participation.

Figure 9 Sampling Bias in Privacy Research



Source: The author.

Incentivization is a driver that introduces pre-selection effects on both sides of the market. In order to extract personal data, firms will probably increasingly offer monetary rewards to individuals for their information. Those who place the highest value on money will be enticed to disclosure as

stated above. Moreover, those who are able to pay the most for the information (or at least a suitable amount) will be able to purchase the data. For all other parties, it holds that they neither have an interest nor the budget to participate in the exchange. The societal consequences of such developments are not well thought through. We cannot assume that the market will automatically be regulated over prices in the presence of network externalities, public good traits, and asymmetric information problems, which are especially pronounced in the markets for personal data.

Relation with PACS development and adoption:

In order to succeed in personal data intermediation markets, businesses need to understand the basic workings and the frictions occurring in these markets. Moreover, they need to better understand under what conditions individuals participate in consumer-direct services and what types of data can be extracted. In addition, the following points are important:

- Neither from surveys nor from experimental evidence, can we expect to obtain wholly unbiased valuations of personal data;
- The incentive-compatibility of mechanisms to extract personal data and to obtain valuations will impact data quality;
- How the decision to disclose information or not is framed will influence the distribution of valuations of personal data; and
- Most mechanisms will lead to skewed distribution of participants. Essentially, this means that data on participants cannot be extrapolated to larger population segments.

References to Chapter III

Acquisti, A., L.K. John and G. Loewenstein (2013). What Is Privacy Worth?, *Journal of Legal Studies*: 42 (2)1 http://chicagounbound.uchicago.edu/jls/vol42/iss2/1

Akerlof, G. and R. Kranton (2000). Economics and Identity, *The Quarterly Journal of Economics* CVX (3): 715-753.

Aperjis, C. and B.A. Huberman (2012). A market for unbiased private data: Paying individuals according to their privacy attitudes, First Monday 17 (5) (May).

Andrade, E. B., V. Kaltcheva and B. Weitz (2002). Self-Disclosure on the Web: The Impact of Privacy Policy, Reward, and Brand Reputation, in *Advances in Consumer Research,* S. M. Broniarczyk and K. Nakamoto (eds.), Valdosta, GA: Association for Consumer Research, pp. 350-353.

Andreoni, J. and R. Petrie (2004) Public goods experiments without confidentiality: a glimpse into fund-raising, Journal of Public Economics 88: 1605– 1623.

Andreoni, J. and R. Petrie (2008). Beauty, gender and stereotypes: Evidence from laboratory experiments, *Journal of Economic Psychology* 29(1): 73-93.

Barmettler, F., E. Fehr and C. Zehnder (2012). Big experimenter is watching you! Anonymity and prosocial behavior in the laboratory, *Games and Economic Behaviour* 75(1): 17-34.

Baumer, D.L., J.B. Earp and J.C. Pointdexter (2005). Quantifying Privacy Choices with Experimental Economics, *infosecon.net/workshop/pdf/16.pdf*

Benjamin, D.J., J.J. Choi and A. J. Strickland (2010). Social Identity and Preferences. *American Economic Review* 100(4): 1913-1928.

Beresford, A.R., D. Kübler, S. Preibusch (2012). Unwillingness to pay for privacy: A flied experiment, Economics Letters 117 (1), 25-27.

Bohnet, I., Frey, B.S., (1999). Social distance and other-regarding behavior in Dictator Games: Comment. *American Economic Review*, 89(1): 335–339.

Buchanan, T., P. Schofield, C.B., Joinson, A.N. and U.R. Reips (2006). Development of measures of online privacy concern and protection for use on the Internet, *Journal of the American Society for Information Science and Technology* 58: 157 – 165.

Campbell, L. Gordon, M. Loeb, and L. Zhou (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. Journal of Computer Security, 11(3): 431–448.

Cavusoglu, H., Mishra, B.& Raghunathan, S. (2004). The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. International Journal of Electronic Commerce, 9(1): 69 – 104.

Charness, G. and Gneezy, U. (2008) 'What's in a Name? Anonymity and Social Distance in Dictator and Ultimatum Games', Journal of Economic Behavior & Organization 68(1): 29–35.

Chellappa, R. K., and Shivendu, S., Mechanism Design for "Free" but "No Free Disposal Services": The Economics of Personalization under Privacy Concerns, *Management Science* 56(10): 1766-1780.

Chen, H., H. Marmorstein, M. Tsiros and A.R. Rao (2012). When More Is Less: The Impact of Base Value Neglect on Consumer Preferences for Bonus Packs over Price Discounts. *Journal of Marketing* 76 (4): 64-77.

Chen, Y., S. Chong, I.A. Kash, T. Moran, and S. Vadhan (2013). Truthful mechanisms for agents that value privacy, in: Proceedings of the fourteenth ACM conference on Electronic commerce, Philadelphia, Pennsylvania, USA, pp. 215-232.

CompassIntelligence (2013).Valuing Identity in Today's Digital World: The Business case for defining digital identity and how to value it correctly, Presentation (July).

Culnan, M. and P.K. Armstrong (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation, *Organization Science* 10 (1): 104–15.

DellaVigna, S. (2009). Psychology and Economics: Evidence from the field. *Journal of Economic Literature* 47: 315-372.

Dinev, T. and Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions, *Information Systems Research* 17(1): 61-80

Dohmen, T., Falk, A., Huffman, D., Sunde, U., Schupp, J., Wagner, G. G. (2011). Individual risk attitudes: Measurement, determinants, and behavioral consequences. *Journal of the European Economic Association* 9 (3): 522–550.

Easley, D. and J. Kleinberg (2010). Networks, Crowds, and Markets: Reasoning about a Highly Connected World, Cambridge University Press.

Egelman, S., A.P. Felt, D. Wagner (2013). Choice architecture and smartphone privacy: There's a price for that, The Economics of Information Security and Privacy, 211-236.

ENISA (2011). Data Breach Notifications in European, Report of the European Network and Information Security Agency, http://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/library/deliverables/dbn

Feri, F., Giannetti, C.,and Jentzsch, N. (2016). Disclosure of Personal Data under Risk of Privacy Shocks, *Journal of Economic Behavior and Organization* 123 (March): 138 – 148.

Fershtman, C., and U. Gneezy (2001). Discrimination in a Segmented Society: An Experimental Approach, *Quarterly Journal of Economics* 116 (1), 351-377.

Gkatzelis, V., C. Aperjis and BA. Huberman (2012). Pricing Private Data, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2146966

Goldfarb, A., and C. Tucker (2012). Shifts in Privacy Concerns. *American Economic Review*, 102(3): 349-53.

Grant, R.W. (2012). Strings Attached Untangling the Ethics of Incentives, Princeton University Press, Cambridge.

Gnesi, S., I. Matteucci, C. Moiso, P. Mori, M. Petrocchi and M. Vescovi (2014). My Data, Your Data, Our Data: Managing Privacy Preferences in Multiple Subjects Personal Data, , in B. Preneel and D. Ikonomou (eds.), Privacy Technologies and Policy, Lecture Notes in Computer Science, Vol. 8450, pp. 154-171.

Hirshleifer, J. (1971). The Private and Social Value of Information and the Reward to Inventive Activity, *American Economic Review* 61, 561–574.

Hirshleifer, J. (1980). Privacy, Its origin, Function, and Future, *Journal of Legal Studies* 9: 649–66.

Huberman, B.A., Adar, E. and Fine, L.R. (2005). Valuating Privacy, *IEEE Security & Privacy* 3(5): 22–25.

Hermalin, B. & M. Katz (2006). Privacy, property rights and efficiency: The economics of privacy as secrecy, *Quantitative Marketing and Economics* 4(3): 209-239.

Jentzsch, N., A. Harasser, S. Preibusch (2012). Monetising Privacy – An Economic Model of the Pricing of Personal Information, ENISA Report, Greece, www.enisa.europa.eu/activities/identity- and-trust/library/deliverables/monetising-privacy.

Jentzsch, N. (2014). Auctioning Privacy-Sensitive Goods: A note on Incentive-Compatibility, in B. Preneel and D. Ikonomou (eds.), Privacy Technologies and Policy, Lecture Notes in Computer Science, Vol. 8450, pp. 133-142.

Jentzsch, N. (2014). Secondary Use of Personal Data: A Welfare Analysis, *European Journal of Law and Economics*, February 2014, DOI 10.1007/s10657-014-9436-1

Jentzsch, N. (2012). Verhaltensexperimente zur persönlichen Privatsphäre erfordern neue Standards, DIW Wochenbericht, DIW Berlin, German Institute for Economic Research: 79(9): 12-14.

Jentzsch, N. (2007). Financial Privacy – An International Comparison of Credit Reporting Systems (Springer-

Verlag, Heidelberg), 2. Revised edition.

Jentzsch, N., G. Sapi and I. Suleymanova (2013). Targeted pricing and customer data sharing among rivals, *International Journal of Industrial Organization* 31(2): 131-144.

Johnson, E.J., Bellman, S. and Lohse, G.L. (2002) Defaults, framing and privacy: Why opting in-opting out, *Marketing Letters*, 13 (1): 5-15.

Kearns, M., M. Pai Mallesh, A. Roth, and J. Ullman (2014). Mechanism Design in Large Games: Incentives and Privacy, *American Economic Review*, 104(5): 431-35.

Koehn, N.F. (2012). When Life is a Bunch of Carrots, The New York Times, February 4, 2012, http://www.nytimes.com/2012/02/05/business/strings-attached-looks-at-incentives-and-ethics-review.html

Krahnen, J.P., Rieck, C. and Theissen, E. (1997) Messung individueller Risikoeinstellungen, Center for Financial Studies Working Paper, www.ifk-cfs.de/fileadmin/downloads/publications/wp/97_03.pdf

Kumaraguru, P. and L.F. Cranor (2005). Privacy Indexes: A Survey of Westin's Studies CMU-ISRI-05-138 December 2005 CMU-ISRI-05-138.pdf

Levitt, S.D. and J.A. List (2007): What Do Laboratory Experiments Measuring Social Preferences Reveal About the Real World? *Journal of Economic Perspectives* 21, 153-174.

List, J. A., R. P. Berrens, A. K. Bohara, and J. Kerkvliet (2004). Examining the Role of Social Isolation on Stated Preferences, *American Economic Review* 94, 741-752.

Malhotra, N. K., Kim, S. S. and Agarwal, J. (2004). Internet Users' data Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model, *Data Systems Research* 15(4): 336-355.

Nettle D., Z. Harper, A. Kidson, R. Stone, I.S. Penton-Voak (2012) The watching eyes effect in the Dictator Game: It's not how much you give, it's being seen to give something, *Evolution and Human Behavior* 34: 35-40.

OECD (2013). Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, OECD Digital Economy Papers, No. 220, OECD Publishing. http://dx.doi.org/10.1787/5k486qtxldmq-en

Plott, C.R., and K. Zeiler (2005). The Willingness to Pay-Willingness to Accept Gap, the Endowment Effect, Subject Misconceptions, and Experimental Procedures for Eliciting Valuations. *American Economic Review* 95 (3): 530-545.

Plott, C.R., and K. Zeiler (2007). Exchange Asymmetries incorrectly interpreted as evidence of endowment effect theory and prospect theory? *American Economic Review* 97 (4): 1449-1466.

Plott, C.R., and K. Zeiler (2011). The Willingness to Pay—Willingness to Accept Gap, the Endowment Effect, Subject Misconceptions, and Experimental Procedures for Eliciting Valuations: Reply *American Economic Review* 101 (2): 1012-1028.

Posner, Richard A. (1981). The Economics of Privacy, *American Economic Review* 71, 405–409.

Preibusch, S. (2013) Guide to measuring privacy concern: Review of survey and observational instruments, *International Journal of Human-Computer Studies* 71 (12): 1133–1143.

Ruths, D. and J. Pfeffer (2014). Social Media for Large Studies of Behavior, *Science* 346 (6213): 1063-1064

Rigdon, M., Ishii, K., Watabe, M., and Kitayama, S. (2009). Minimal social cues in the dictator game. *Journal of Economic Psychology* 30, 358-367.

Roth, A. (2012). Buying Private Data at Auction: The Sensitive Surveyor's Problem, *ACM SIGecom Exchanges* 11(1): 3-8.

Rothschild, M. and J.E. Stiglitz (2001). Competition and Insurance Theory Twenty Years Later, *Geneva Papers on Risk and Insurance Theory* 22 (2): 73-79.

Schultze-Melling, J. (2014). Datenschutz messbar und vergleichbar Machen – Von Metriken, Reifegraden und Key Performance Indicators, 15. Euroforum Datenschutzkongress, Berlin.

Smith, J.H., Milberg, S.J., & Burke, S.J. (1996). Information privacy: Measuring individuals concerns about organizational practices. *MIS Quarterly* 20, 167–196.

Stewart, K. A. and A.H. Segars (2002). An empirical examination of the concern for information privacy instrument. *Information Systems Research* 13, 36–49.

Stigler, G.J. (1980). An Introduction to Privacy in Economics and Politics, *Journal of Legal Studies* 9: 623–44.

Stole, L. (2007). Price Discrimination and Competition, in M. Armstrong and R. Porter: Handbook of Industrial Organization, Volume 3. Amsterdam: Elsevier, pp. 2221-2299.

Sholtz, P. (2001). Transaction Costs and the Social Costs of Online Privacy, *First Monday* 6(5) URL: http://firstmonday.org/issues/issue6_5/sholtz/index.html

Tsai, J.Y. S. Egelman, L. Cranor and A. Acquisti (2011). The Effect of Online Privacy Information on Purchasing Behaviour: An Experimental Study, *Information Systems Research* 22(2), pp. 254-268).

World Economic Forum (2011). Personal Data: The Emergence of a New Asset Class, Report, http://www.weforum.org/reports/personal-data-emergence-new-asset-class

Xiao, D. 2013. Is privacy compatible with truthfulness? In ITCS, R. D. Kleinberg, Ed. ACM, 67–86.

Zhang, J. (2011). The Perils of Behavior-Based Personalization, *Marketing Science* 30 (1): 170-186.

IV. Policy Instruments Impacting on PACS Adoption

4.1 Policy Instruments Impact on Cost-Benefit Trade-offs in Cyber-Security

There are a number of policy instruments (incentive schemes) that alter the underlying cost-benefit trade-offs, thus impacting the economic incentives of market participants. Some of these measures provide a changed allocation of responsibilities and liability in order to incentivize greater cyber-security, others alter the distribution of critical information in the market by implementing information sharing. Policymakers should answer the question first whether prices provide the correct signals in order to achieve the goal intended. Moreover, they should be aware of the following:

- Instead of using one instrument, there might be a ***combination of instruments*** that is more effective;
- ***Systematic impact assessments*** are a necessary condition in order to obtain a clear understanding of the effectiveness of the instrument; and
- Government needs to provide the right level of incentivization (for example, the size of a tax credit granted) in order to improve cyber-security.

At the highest level, market-conforming and non-conforming measures need to be differentiated. Non-conforming measures are quantity and/or price restrictions. These result in a dysfunctional price mechanism and are not discussed here. Among the market-conforming measures, there are measures that are either typically mandatory or typically voluntary. However, there are also measures that can be implemented as both. **Table 10** describes the instruments. In the following, we will only summarize these incentive schemes and the challenges for policy makers that arise with their implementation. This is by no means a complete list and/or evaluation, as this is not the main purpose of this paper.

Table 10 Instruments that Impact on Incentives of Market Participants

Character	Instrument
Mandatory	Adjustment of liability of firms for duty of care / diligence
	Data breach notifications
	Install and clarify property rights to personal data
Mandatory or voluntary	Trust marks and technical security seals
	Information sharing of incidence information
	Promotion of cyber insurance
	Care and diligence standards
Voluntary	Privacy by design and security by design
	Increased tax credit for cyber-security investments
	Accelerated cost recovery reductions on cyber-security investments
	Funding of research projects at firms
Other measures	Establish personal data as economic valuable, which becomes a object of negotiation among transaction partners
	Increase consumer education with regard to data protection/privacy, increase awareness of risks
	Educational measure to create risk awareness among firms

Source: The author.

4.1.1 MANDATORY INSTRUMENTS AND INCENTIVE SCHEMES

Mandatory instruments are implemented through legislation, regulation or mandatory Codes of Conduct. Based upon these instruments market players can be held liable for their actions.

Adjustment of duty of care liability: Entities that qualify as banks fall under a number of banking regulations, among them duty of care or diligence standards. Likewise, firms that qualify as a Critical Infrastructure Organization (CIO), for example energy and telecom firms, could fall under specific diligence standards for cyber-security. Similar to the approach applied in banking, such rules would not prescribe specific security technologies, but rather give authorities the tools to assess the processes and strategies adopted by a CIO to address cyber-security threats. The threats of criminal sanctions or fines would provide an incentive for these companies to improve their IT security. The challenge for policy makers is to design these incentives under conditions of correlated risks, i.e. scenarios of interdependent risks like in cloud computing.

Data breach notifications: In Europe mandatory data breach notifications were introduced for telecoms and Internet Service Providers in 2009 with the E-privacy Directive. These regulated firms in these industries must notify individuals about security breaches if they may result in identity theft, fraud, physical harm, humiliation, or damage to reputation. The EU is discussing whether to expand the scope to all sectors (including financial services). Requiring data breach notifications, regardless of sector, leave the consumer better informed about security issues at service providers he/she is dealing with. However, it could also lead to a flooding of notifications and, consequently, consumer

desensitization. When data breach notifications are made public, firms have an incentive to decrease reputational damage incurred due to such reporting. Moreover, if data breach notifications are made mandatory, the picture becomes more complete compared to regimes where reporting is voluntary.

Install property rights to personal information: One of the most controversial areas in the privacy literature is whether it makes sense to install property right to personal data. In general, property rights would ensure that information is owned by the data subject and can be traded. For this to work, however, property rights need to be clarified and individuals need to have an idea about the economic value of their data. This is challenging for policy makers as it might (1) not fit the traditional legal approach of data protection; and (2) the economic value of personal information is difficult to establish.

4.1.2 MANDATORY OR VOLUNTARY INSTRUMENTS AND INCENTIVE SCHEMES

Trust marks and technical security seals: The display of an online seals is already widespread on the Internet. Examples include TRUSTe, BBBOnline, EuroPrise, and the UDL Datenschutz-Gütesiegel. These seals can be obtained voluntarily by the firm wanting to display them. Potentially, they could be made mandatory for CIOs. While the seals allow for the signalling of improved security, it is unclear if they translate into a competitive advantage (i.e. increase sales or reduced customer switching). Moreover, once a market for private certification is established on an EU-wide basis, the multitude of seals could lead to a confusion of end-users, even as seals are supposed to guide consumers when making purchases.[43] Policy makers would need to assess the effects of seals first, before obliging firms to obtain such certification.

Information sharing of incidence information: One instrument to improve cyber-security is the sharing of critical incidence information (intrusions, viruses, warnings). However, information sharing often also involves activities of an educational nature, like peer-to-peer exchanges and advice. There are variations of how this is done across EU Member States. One mechanism is the Computer Emergency Response Teams (CERTs), also known as Computer Security and Incident Response Teams (CSIRTs). Other mechanisms include informal exchanges and community-driven Warning, Advice and Reporting Points (WARPs).[44] Policy makers are faced with the challenge that there might be a lack of cooperation between stakeholders and/or with LEAs; as well as a lack of incentives to report information. Moreover, there might be a lack of incentive to report reliable data.[45] If not designed properly (for example, establishing reciprocity), information sharing can invite free-riding where some participants learn much but share little (Gordon 2007).

Promotion of cyber-insurance: Insurance companies offer the assessment of a firm's risk culture. This includes vulnerability of information systems, networks and processes, as well as of liability in cases of data breaches and losses, IP infringement or defamation. Insurers also estimate the

[43] ENISA (2013). On the security, privacy and usability of online seals, https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/on-the-security-privacy-and-usability-of-online-seals

[44] See for a more detailed explanation: http://www.enisa.europa.eu/activities/cert/background/coop/terms-definitions-1/warps

[45] Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions (2013). Cyber-security Strategy of the European Union: An Open, Safe and Secure Cyberspace, http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

probability of future IT damages based upon current security mechanisms. Cyber-insurance is currently a small, but growing, market segment with the potential to help improve cyber-resilience due to a better allocation of risks among market players. Insurance schemes as risk-transfer mechanisms could potentially also be made mandatory (such as in car insurance) for firms that are CIO, for example, or firms that hold large databases of data. Policy makers face the challenge of jump-starting the market for cyber-insurance. As long as cyber-security is not a high priority at management level and there are no significant fines for data breaches, firms have no incentive to purchase cyber insurance. The Commission has invited stakeholders to develop harmonize risk metrics.[46]

Care and diligence standards: Security standards can be established to be used either voluntarily by stakeholders or on a mandatory basis. In the latter case, firms would only be allowed to operate in the market once they adhere to the standards. Many standards systems, however, are voluntary. ENISA has drawn up a list of standards relevant for telecom operators, including ISO, ITU and other standards (ENISA 2012). Standards can guide the industry to improve on their security features and to make systems more inter-operable. However, they can also create market-access barriers if too high and if mandatory. The challenge faced by policy makers is to allow sufficient flexibility that higher security standards may eventually surpass lower ones and that standards do not unduly disadvantage smaller players.

Open questions regarding instruments that impact economic incentives:

- There is no systematic overview of how costly the individual instruments are when applied to the private sector;
- There is no systematic evidence of how effectively the instruments shift the cost-benefit trade-offs of players; moreover, the instruments have to be assessed based upon their effectiveness in a networked world;
- There is no ranking of instruments that the private sector players would prefer;
- There is no systematic analysis of how these instruments interact with each other and whether the adoption of a specific combination might improve effectiveness; and
- With respect to individual instruments, it is often unclear whether it should be made mandatory and/or what the right level of establishment is to provide a proportional response to the possible risks.

[46] Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions (2013). Cyber-security Strategy of the European Union: An Open, Safe and Secure Cyberspace, http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

References to Chapter IV

ENISA (2012). Shortlisting network and information security standards and good practices https://resilience.enisa.europa.eu/article-13/shortlist-of-networks-and-information-security-standards

Gordon, L.A. (2007). Incentives for Improving Cyber-security in the Private Sector: A Cost-Benefit Analysis, http://hsc-democrats.house.gov/SiteDocuments/20071031155020-22632.pdf

V. New Models of Cyber-security and Privacy Economics

The research on the economics of cyber-security and privacy contributes to a better understanding of the frequent failures to protect information systems and sensitive data. However, much needs to be done in order to derive more robust insights that are better generalizable to different situations and populations. We need in particular much more basic research on strategic privacy behaviour of individuals.

Cyber-security Economics: Summary of Potential Action Points

Guidance and Advice for PACS firms:

(a) There should be more guidance on models and cases for cost-benefits analyses of IT security investments for firms planning to invest in PACS technologies and the same holds for the provision of more standardized tools to assess risk inherent in current IT systems;

(b) There could some value-added in the development of a toolbox for PACS firms to enable them to systematically present to targeted end-users the value proposition of the PACS they developed; and

(c) There is a critical need for more evidence-based advice, i.e., experimental analyses with respect to consumer behavior after security breaches, thus enabling IT staff to showcase the costs of bad reputation through data breach events.

Guidance and Advice for Policymakers:

(d) There needs to be a more systematic overview showing how costly the individual instruments for the facilitation of adoption of PACS and PACS frameworks are;

(e) There is no systematic evidence of how effectively the instruments shift cost-benefit trade-offs of players, moreover, the instruments have to be assessed based upon their effectiveness in a networked world;

(f) There is no ranking of instruments that private sector players would prefer and no systematic analysis of how these instruments interact with each other and whether the adoption of a specific combination might improve effectiveness;

(g) With respect to the individual instrument to further PACS adoption, it is often unclear whether it should be made mandatory and/or what the right level of establishment is to provide a proportional response to the risks encountered; and

(h) There needs to be more sourcing of knowledge (in terms of research) on interconnected risks and mutual exposures as well as spill-over effects of security incidents.

Privacy Economics: Summary of Potential Action Points

As new PACS innovations develop quickly, it is imperative to accompany these developments with robust new models of cyber-security and privacy as well as robust incentive schemes. Not only will Europe be better equipped to manage the risks that are on the horizon, but it can also reap the benefits associated with technological developments, such as cloud computing, Big Data Analytics, mobile social networks and biometric identification.

Guidance and Advice for PACS firms:

(a) ***Understanding the market:*** PACs developers ought to consult the IPACSO framework in order to better understand the market they will enter with their product; and

(b) ***Privacy-risk assessment:*** More guidance needs to be given on the assessment of privacy risk in companies and the value of privacy risk indicators as well as a correct loss estimation from privacy breaches;

Future Research Areas:

(c) ***Privacy preferences:*** Basic research is needed on privacy preferences related to the different types of transactions, such as incentivized information transactions compared to incentivized composite transactions. There should be also less emphasis on self-reported data;

(d) ***Functional form of privacy costs:*** More research effort needs to be devoted to the reliable estimation of privacy costs and to assess the shape of the privacy cost functions;

(e) ***Elicitation mechanisms:*** There needs to be the development of better methods to gauge valuations of personal data. Neither from surveys nor from experimental evidence can we expect to obtain wholly unbiased valuations. Most mechanisms will lead to skewed distribution of participants, if they are not differentially private;

(f) ***Behavioral foundations:*** More effort must be invested in the development of mechanisms for the intermediation of personal data that are based upon behavioral research. Compensating individuals for privacy concerns is a workable approach only in the case, where privacy concerns can be identified in a reliable way;

(g) ***Priming and framing of privacy decisions:*** More attention and research needs to be devoted to the priming and framing of the decision to disclose information and its influence on the distribution of valuations of personal data; and

(h) ***Natural experiments:*** Much more effort needs to be invested in incentivizing the industry to cooperate with researchers on natural experiments in the field, where priming on privacy is reduced, if not even absent. There ought to be much less emphasis on surveys on privacy in future.

New Models for Cyber-security and Privacy

Methods, Models and Theories: Behavioural Models, Networks and Action Research

Methodological advances in cybercrime and privacy economics: The most important field will be basic research to develop better methodologies to capture and analyse problems in the economics of cybercrime. However, these methods need to adhere to scientific and ethical standards; they also should advance the quality of research produced in the fields. Policymakers ought to rely less on self-reported data in surveys and more on action-based research, where actual behaviour of firms and consumers is observed. The methods that should be further developed are laboratory and field experiments of cybercrime, privacy and identification, modelling estimation techniques for security and privacy decision-making, Big Data Analytics, and methods such as event studies. It is advised to focus first on this area, as the methodological advances will influence the quality of research produced.

Behavioural models of cybercrime and privacy economics: It is recommended to work with behavioural models as well as new mental models of cybercrime and privacy. These works ought to validate utility models that integrate more than the maximization of monetary payoff; namely social preferences such as reputation. In addition, ways of introducing ambiguity in decision-modelling should be found. Finally, more effort needs to be spent analysing threats posed by social engineers and disgruntled workers, which will become an important part in the development of behavioural cybercrime analytics.

Models of interdependency problems: Another important trend is the research on interdependency problems, as captured in network analysis. The application of network modelling to problems of cybercrime and privacy is only at beginning stages. However, much more can be learned by identifying network effects and the indirect impact of cybersecurity and privacy decisions by stakeholders in the market.

Empirical modelling of cybercrime and privacy problems: There is an urgent need to improve the empirical base upon which research works. This request ties in with the above statement to rely less on reported statements and more on observations of actions in a natural environment. Here, policy makers ought to strengthen research cooperation with the private industry to facilitate natural experiments. Moreover, policymakers ought to strengthen and clarify the position of researchers who engage in one way or the other for research purposes in cybercrime activities. Such research can advance our empirical foundations and help to better identify vulnerable populations.

Economic Incentives of PACS adoption and interaction with instruments: As discussed in-depth in this report, we need a more comprehensive overview of the different instruments to influence the economic incentives of players to adopt PACs. Also more attention needs to be devoted to the study of the interaction of these different instruments and whether their effects could be enhanced by using social multipliers.

More robust research methods will lead to more reliable research insights. A more efficient transfer of such insights could enable greater resilience of critical infrastructures by enhancing economic incentives to adopt and invest in innovative PACs.

ANNEX Overview Table

Cybercrime and Data Breach Surveys and Research	Issuer/ Author	Pub. Date	Research Area	Survey?	Survey population or database	Time series available	Some results
Cost of Data Breach Study: Germany	Symatec / Ponemon	2013	Germany	yes	31 firms in 11 diff. industries	2008-2013	Data breach costs increased since 2008
Cost of Data Breach Study: Global	Symatec / Ponemon	2013	Global	yes	277 (2012) / 199 (2011) firms/orgs in 9 countries	2011-2012	Data breach costs increased in 2011-2012
Internet Security Threat Report	Symantec	2014		yes	Vulnerabilities database of Global Symantec Network	2011-2014	The total number of breaches in 2013 was 62 percent greater than in 2012 with 253 total breaches. It was also larger than the 208 breaches in 2011.
2012 Norton Study: Consumer Cybercrime Estimated at $110 Billion Annually	Symantec / Norton	2013	24 countries	yes	13.000 adults in 24 countries	2011-2012	1.5 million victims daily, price tag on crime: 110 billion USD
2013 McAfee The Economic Impact of Cybercrime and Cyber Espionage	McAfee	2013	Global	no	Estimations of costs	no	A USD 400 billion loss due to cybercrime—the high end of the range of probable costs—would be a fraction of a percent of global income.
McAfee Threat Reports (Quarterly Report), First quarter 2013	McAfee	2013	Global	no	McAfee Global Threat Intelligence Network	2009-2013	All malware tracked by McAfee -affecting clients, servers, networks, mobiles stands at more than 128 million samples.
2013 Data Breach Investigations Report	Verizon	2013	Global	yes	19 global organizations	2009-2013	37% of data breaches affect financial orgs, 24% occur in retail & restaurants, 20% affected network such as utilities and transportation.
Microsoft Security Intelligence Report	Microsoft	2013	Global	yes	105+ locations	2007-2013	Trends and insights on security vulner-abilities, exploit activity, malware and potentially unwanted software, spam, phishing, malicious websites, and security trends from 105+ locations around the world

Cybercrime and Data Breach Surveys and Research	Issuer/ Author	Pub. Date	Research Area	Survey?	Survey population or database	Time series available	Some results
Detica Cost of Cybercrime	Detica together with Cabinet Office	2011	UK	no	Public sources	no	Our assessments are, necessarily, based on estimates and assumptions rather than specific examples of cybercrime, or from data of a classified or commercially-sensitive origin.
Kaspersky Security Bulletin 2013	Kaspersky Lab Global Research & Analysis Team	2013	Global		Population of Kaspersky Products	2007-2013	According to KSN data, in 2013 Kaspersky Lab products neutralized 5 188 740 554 cyber-attacks on user computers and mobile devices.
Identity Theft Surveys							
2013 Identify Fraud Report	Javelin Strategy & Research	2013	U.S.	yes	Survey of a representative sample of 5,249 U.S.	2005-2012	2012 identity fraud incidents increased by more than 1 million victims, damage $21 billion, the highest amount since 2009
Consumer Sentinel Network Data Book	Consumer Sentinel /FTC	2007	U.S.	no	Consumer Sentinel, complaint database of FTC	2009-2013	The CSN received over 2 million complaints (excluding do-not-call) during calendar year 2013: 55% fraud complaints; 14% identity theft complaints; and 31% other types of complaints.
2012 Consumer Sentinel Network Data Book	Consumer Sentinel /FTC	2012	U.S.	no	Consumer Sentinel, complaint database of FTC	2008-2012	Rising ID theft complaints since 2001, time series and numbers are available in report
Global Trust and Safety Report	PayPal	2008	US, UK, CA, FR, GER, SP	yes	6,000 online shoppers	2008	Identity theft is more pronounced in English speaking countries. 1 in 10 online consumers in Canada, the UK and the US have been victims of ID theft. Only about 1 in 20 are ID theft victims in France, Germany and Spain.
UK Cybercrime Report 2009	Garlik	2009	UK	yes	unclear	2006-2009	It is estimated that there were 92,000 cases of online identity fraud during 2006.

Source: The author.

This page is intentionally left blank.