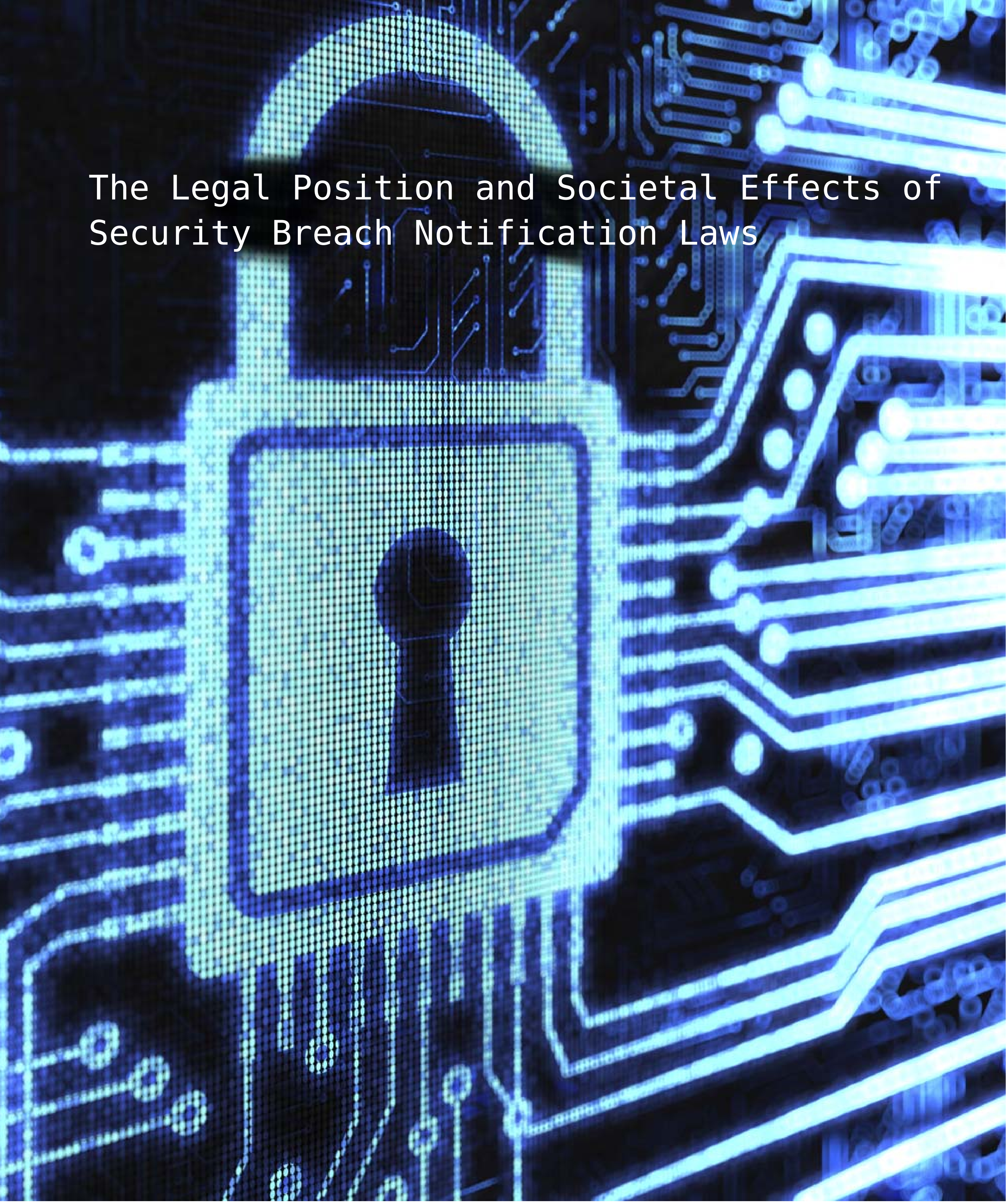
The Legal Position and Societal Effects of Security Breach Notification Laws



Master Thesis
Bernold Nieuwesteeg
August 2013

TU Delft Delft University of Technology
Utrecht University

The Legal Position and Societal Effects of Security Breach Notification Laws

Faculty of Technology, Policy and Management

MSc Systems Engineering, Policy Analysis and Management

<u>Graduation committee</u>
Chairman: Prof. Dr. M.J.G. van Eeten
Professor Governance of Cybersecurity
1st supervisor: Dr.ir. B.M. Steenhuisen
Assistant Professor at the research group Policy, Organization, Law and Gaming
2nd supervisor: Dr.ir. J. van den Berg
Associate Professor at the research group Information and Communication Technology

Faculty of Law, Economics and Governance

LLM European Law

<u>Graduation committee</u>
Graduation supervisor: Dr. S.A. de Vries
Associate Professor at the Europa Institute; Jean Monnet Chair in EU Single Market Law & Fundamental Rights
Second reader: Dr. A. van den Brink
Associate Professor & Director at the Europa Institute

Master Thesis
Author: B.F.H. Nieuwesteeg BSc LLB
Email: Bernoldnieuwesteeg@gmail.com
August 2013

This thesis is written in Cambria. Cambria was designed by Dutch typographer Jelle Bosma in 2004, with Steve Matteson and Robin Nicholas. It is specifically designed to be esthetically pleasing at relatively small sizes, which might facilitate the reader to achieve enhanced thought experiments.

Executive summary

This thesis scrutinizes the proportionality and describes the subsidiarity of proposals for security breach notification laws (hereafter: SBNLs) in the European Union. An SBNL obliges that a security breach within a company or government must be notified to affected customers and a supervisory authority. A law stands the proportionality test if the requirements of effectiveness and necessity are met.[1] Effectiveness means that there is a causal relationship between the measure and the aim pursued. Necessity means that no less restrictive policy options are available that achieve the same aims.[2] The closely linked subsidiarity test assesses the necessity of the *European Union* approach: the question whether the aims of the SBNL and cybersecurity cannot be achieved sufficiently by the Member States *individually*.[3] Subsidiarity is to a great extent a political question and consequently described more limitedly.

Why these tests? Proportionality and subsidiarity are fundamental principles of EU law. They demand the European legislature not to go beyond what is necessary to attain the objectives in the Treaties and to only adopt measures if a European Union approach has added value. The European Court of Justice scrutinizes whether European legislation is in accordance with these principles.

The laws that have been assessed are Article 31 of the proposed Data Protection Regulation (hereafter: PDPR) and Article 14 of the proposed Cybersecurity Directive (hereafter: PCD).[4] Article 31 PDPR concerns a single uniform personal data breach notification obligation. A personal data breach entails the unauthorized access to and/or theft of personal data. Article 14 PCD concerns the harmonization of national (significant) loss of integrity breach notification obligations.[5] A loss of integrity concerns the loss of control over computer systems. A personal data breach always entails a loss of integrity, but a loss of integrity can also occur without the loss of personal data. The aim of the SBNL in the PDPR is "to ensure that individuals are in control of their

[1] Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* [2010] ECR I-0000.

[2] Damian Chalmers, Gareth Davies and Giorgio Monti *European Union Law* (second edition, Cambridge University Press 2010) 362. There is also a third criterion, proportionality strictu sensu, which is sometimes mentioned separately, see section 3.2.1 of this research.

[3] See also Protocol (No 2) on the Application of the Principles of Subsidiarity and Proportionality [2007] OJ C-310/207; Paul Graig and Gráinne de Búrca, *EU Law - Text Cases and Materials* (fifth edition, Oxford University Press 2011) 95.

[4] European Commission 'Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data' (Proposed Data Protection Regulation) COM (2012) 11 final; European Commission 'Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union' (Proposed Cybersecurity Directive) COM (2013) 48 final.

[5] A Dutch initiative for an SBNL focusing on loss of integrity will be discussed extensively in this thesis.

personal data and trust the digital environment"[6] in order to "increase the effectiveness of the fundamental right to data protection".[7] The aim of the SBNL in the PCD is: "to create a culture of risk management and improve the sharing of information between the private and public sectors."[8]

The subsidiarity question covers cybersecurity in general and SBNLs in particular. The Commission argues that a *European* cybersecurity approach is necessary because of the cross border aspect of the Internet, the necessity of a uniform secure Internet for the Single Market and the protection of fundamental rights. Indeed, there is European cybersecurity legislation and a European cybersecurity policy framework. Regarding the PDPR and the PCD in particular, the Commission argues that there is a need to harmonize national initiatives in order to create a level playing field, legal certainty and lower administrative burdens for companies to notify. A literature review in this thesis shows that the United States aims to replace a state level SBNLs by a federal SBNL. The obligation to comply simultaneously with multiple SBNLs caused significant administrative burdens for companies. This strengthens the conception that SBNLs can better be achieved at a European level, although this remains a political consideration. From an apolitical point of view, this thesis did not find a convincing argument about the inappropriateness of a *European* approach regarding cybersecurity and SBNLs.

The proportionality test contains two elements. The first element of the proportionality test, the effectiveness test, is performed more extensively in this thesis than the Commission did in its impact assessment of both the PDPR and the PCD. Legal scholars and the European legislator, usually assess the first aspect of proportionality limitedly.[9] In the PDPR and PCD, the Commission did not mention in what way the SBNL is suitable to achieve the aim "to ensure that individuals are in control of their personal data and thrust in the digital environment" and "to create a culture of risk management and improvement of information sharing between private and public parties". This is a deficiency in the analysis of legislation.

This thesis challenges the aforementioned assumption that determination of causality is straightforward. This is done by a more substantive assessment of the proportionality test. This thesis contributes an empirical study from a security economics perspective, in order to substantively review (the complexity of) effects of SBNLs. Do the (expected) effects of SBNLs match the aims it should attain according to the European proposals?

[6] European Commission 'Impact Assessment accompanying (proposed) Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data' (Impact Assessment of the Data Protection Regulation) SEC(2012) 72 final, section 5.3.1.

[7] Ibid.

[8] European Commission 'Impact Assessment accompanying the Proposal for a Directive of the European Parliament and of the Council Concerning measures to ensure a high level of network and information security across the Union' (Impact assessment of the Cybersecurity Directive) SWD (2013) 32 final, section 6.1.

[9] See for instance Jan H Jans, 'Proportionality Revisited' (2000) 27(3) *Legal Issues of Economic Integration* 239, 240 and section 1.2 of this research.

And are these effects desirable? Legal impact assessments can benefit from this perspective, because knowledge about the effectiveness of the law will be enhanced.

To structure the empirical study, a first and second order effect of SBNLs have been distinguished. The first order effect is the effect of (characteristics of) SBNLs on the amount of breach notifications. Generating notifications is not one of the final aims of the proposed legislation, but a means to achieve the second order effect. The second order effect includes the positive and negative effects of the law on society. A literature review is conducted to provide an overview of what is already known concerning those two effects. The quantitative analysis systematically assesses the first order effect of American SBNLs by a longitudinal dataset containing security breach notifications. The subsequent qualitative analysis reviews the perception of Dutch security experts and managers regarding the first and second order effect and outcomes of the quantitative analysis.

The results can substantiate the first element of the Commissions' proportionality test of European SBNLs:

This study proves the first order effect empirically by means of analyzing American data. The laws have an effect on the amount of breach notifications. The effect is relatively large: a notification increase of at least 50% can be attributed to the law, by a fixed effects regression analyzing differences in breach notification before and after the introduction of the law. The database is partly constructed by underlying sources that only register officially notified breaches, which can explain this high relative increase. From an absolute perspective, the effect is minor: less than 0.05% of the companies notified a security breach in America in the eight-year period that was researched. To compare: a recent study in the United Kingdom published that 88% of the companies surveyed had experienced data theft in 2009. The low absolute number of breaches could be explained by the incompleteness of the dataset, high compliance costs for a company due to reputation damage and unawareness of breaches. The introduction of the law thus has a structural first order effect, at least in the database of known security breaches. It is however ambiguous which aspects of the law cause this effect. Literature review and qualitative analysis showed that enforced sanctions generate compliance with the law and that reputation damage is a major driver for non-compliance. Confidential treatment of the notification and benefits from information sharing about security breaches are perceived as minor incentives for compliance. The quantitative analysis only confirmed that some American laws qualified as strict by American Attorneys cause an increase in notifications, but it is ambiguous what exactly makes these laws strict.

The literature review and the qualitative study demonstrated several positive second order effects perceived in literature and by security managers and experts, such as increased investments in security, fostered cooperation between companies (literature only), increased awareness of consumers of security breaches and faster risk mitigation. The first two effects match with the aim of the PCD to 1.) create a culture of risk management and 2.) enhance information exchange between the private and public sectors respectively. The last two effects correspond with the aim of the PDPR to enhance personal data control of individuals. However, the positive effects can be nuanced. The security managers interviewed already shared security information with competitors, and did not see an incentive for cooperation with the government following from a security breach notification, because they did not value the government as a center of expertise. Moreover, a security expert challenged the effect of increased investments in security because the law provides an incentive to notify, not to improve security practices. Accepting the 'risk' of a notification might be less expensive than improving security practices in order to avoid notifications. This is however not confirmed in literature review or by other qualitative analysis, which implicates that the risk of not providing incentives to improve security practices at all must be perceived as low. Lastly, an increased number of security breach notifications might result in an overload of information that could also result in disinterest and a notification fatigue instead of enhanced awareness and risk mitigation.[10] This overload is not a big treat given the current low amount of notified security breaches. For instance, in America, about 600 million records were breached in the eight-year period observed.[11] This would entail that, on average, an American citizen would be notified twice in eight year.

Hence, the second order effects in literature and qualitative analysis, although they are perceptions that can be nuanced, do match the objectives pursued in legislation. But, the objectives are vaguely defined and while their attainment could constitute effectiveness in the legal sense, the question remains what makes an SBNL effective and when an SBNL is effective. Moreover, there are also additional negative effects associated with SBNL in literature and qualitative analysis, such as reputational costs and maintenance costs. The effects of SBNLs and their relation with the aims of legislation are mapped in table 1.

Effects	**Order**	**Lit**	**Qual**	**Quan**	**Relation with legislation**
Enforced sanctions	1st	V	V	X	
Reputational damage		V	V	-	
Appropriateness		V	V	-	
Benefits inf. sharing		V	V	-	
Confidential treatment		X	V	-	
Overall first order effect		-	V	V	
Faster risk mitigation	2nd (positive)	V	V	-	Aim PDPR: enhance personal data control of individuals.
Increased awareness consumers		V	V	-	Aim PDPR: trust in the digital environment
Increased security investments		V	V	-	Aim PCD: create a culture of risk management
Fostered cooperation		V	X	-	Aim PCD: enhance

[10] *Impact assessment PDPR* (n 6), section 14.3.1 under 4).
[11] The three largest breaches in the United States database contain 300 million records, see chapter 5.

					information exchange between the private and public sectors
Reputational costs for companies	2nd (negative)	V	V	-	
Compliance costs for companies		V	V	-	(Only) compliance costs are estimated by the Commission
Maintenance and processing costs for Member States		V	-	-	
Costs of increased investments and cooperation for companies		V	-	-	
Notification fatigue for consumers		V	-	-	-Aim PDPR: enhance personal data control of individuals. -Aim PDPR: trust in the digital environment
Incentive to notify, not to improve security for companies		-	V	-	Aim PCD: create a culture of risk management

Table 1: effects of SBNLs (V=proved or mentioned; X=disproved; "-" = not researched)

The second element of the proportionality test concerns the question whether there are less restrictive equally effective measures available. The SBNL can restrict companies, because it infringes the fundamental freedom to conduct a business by imposing administrative, compliance- and reputational costs.[12] This study offers two observations concerning this infringement.

First, the freedom to conduct business is more infringed than the Commission states. The cost assessment of the Commission only included the costs of making a notification, which are estimated between 125 euro and 20000 euro per notification. But, literature and qualitative analysis showed that there are costs that the Commission did not take into account, such as the reputation damage incurred (estimations up to 2% of a company's turnover) and the costs of processing and enforcement of breach notifications. The cost estimation of the Commission thus is undervalued compared with the total societal costs of an SBNL.

Second, the coexistence of the PDPR and the PCD unnecessarily infringes the freedom to provide a business as it imposes unnecessary costs for companies. In many cases, a breach thus should be notified twice to both the European supervisory authority and to

[12] See also within the context of Case C-70/10 *Scarlet Extended v SABAM* [2011] ECR I-0000, discussed in section 3.2.2 of this research. The freedom to conduct business can be infringed by imposing unnecessary administrative burdens.

the competent national authority, because the scope of personal data loss and loss of integrity overlap.[13] Second, the proposals are regulated by a different legal instrument and emit different signals. The confidential treatment in the PCD will not function properly if simultaneously companies are forced to publicly disclose the same information in the PDPR.

To conclude, the fuzziness of the aims and the complexity of measuring effects hamper the determination of a reasonable expectation of causality between the measure and the aims pursued. The Commission sets aims that are fuzzy and hard to measure, and does not specify how these goals will be achieved through the adoptions of SBNLs. Likewise, the empirical measurement of effects in part β showed that it is complex to pinpoint effects of SBNLs. Moreover, the Commission undervalued societal costs and adverse effects.

In my view, in the current situation, a reasonable expectation of effectiveness is not demonstrated sufficiently. In the theoretically desired situation, the goals are clear and measurable. The law is effective because the measurable aims are achieved by the measure. But, still, effectiveness is not simply attaining aims. Even if the causal relation between the measure and its aims can be proved in a narrow sense, the question remains whether the achievement of these aims is effective.

From a security economics perspective, it can be argued that the law is effective if the revenues of positive effects are higher than the societal costs of negative effects.[14] This requires an accurate empirical measurement of these effects, initiated in part β, and a quantification of these effects. Unfortunately, this approach towards effectiveness does not cover non-economic, non-measurable aims such as the protection of fundamental rights. The protection of fundamental rights is not always 'efficient' and can certainly not always be quantified, but European legislation must remain within the boundaries of fundamental rights.[15] Moreover, the complexity of the legal interferences in the field of cybersecurity makes it impossible to provide an exhaustive balance sheet of all (expected) effects. A security economics perspective would not be the perfect means to define effectiveness, because some aims are not measurable and expected effects are complex.

Both a legal and an economic approach do not provide an optimal outcome for the definition of 'effectiveness'. There is no uniformity of what makes a law effective. Thus, still the effectiveness question remains. What is needed to determine the effectiveness of SBNLs? Who may decide when a law is effective? In a democracy, we all should decide. More concrete: the European Commission, Parliament and Council state *ex ante*

[13] The severity of this unnecessary burden depends on the extent to which the two administrative systems that process breach notifications cooperate.

[14] See table 1, effects of SBNLs. One could also argue that only a *pareto improvement* of a positive effect would be preferable.

[15] In countries such as China, where there is more limited attention for fundamental rights, governmental policies, for instance the construction of a highway, can be executed far more efficiently than in the European Union.

in the ordinary legislative procedure the aims of the law. The European Court of Justice decides *ex post* whether the law is effective. Thus, effectiveness in redefined, as legal and economic approaches towards effectiveness are troublesome. This definition must be regarded as a starting point for further research on interpreting effectiveness of the law.

Effectiveness is the causality between a legislation and its aims defined by a democratic decision making process where as much information as possible about (potential) positive and negative effects is provided.

Hence, taking this definition into account, improving information about potential positive and negative effects is the key tool to enhance effectiveness of the law and correctly assess its necessity. The executed empirical analysis in this thesis has provided knowledge about the effects of SBNLs that can be used by the Commission. Increased availability of information about societal impact (expectations) enhances decision making of the legislature *ex ante* and the scrutiny of the Court *ex post* that determine the proportionality of cybersecurity laws. The Commission, which has the power of initiative, should invest to provide this information.

To conclude, additional information about effects of legislation on society will improve the quality of draft legislation and the judicial decision about proportionality. For example, information about the adverse reputation damage on companies, demonstrated in this thesis, will play a vital role when judging about the infringement on the freedom to conduct business. Additional information about effects will not be decisive in a judicial decision, since also non measurable effects need to be balanced and (expected) effects have a certain margin of error. The proportionality test as such must be seen in relation to these inherent flaws within measuring effectiveness of the law on society. Often, causality between the measure and the aim can and will not be 'proven' scientifically by the legislature and the Court. Nevertheless, the proportionality principle has been a corner stone of European Law to analyze the effectiveness and necessity of legislation. Further enhancement of the execution of this principle by improving information about societal effects increases the democratic legitimacy of European Union law.

Therefore, this thesis recommends the European Commission to enhance information about effects. This can be done to improve the measurement of (the expectation of) effects before and after the adoption of the law. These recommendations can be used for improving European laws in general and the PDPR and PCD in particular.

Before the adoption of the law, a reasonable expectation of effectiveness should be provided by the Commission. This entails the operationalization of measurable aims, the separation of non-measurable aims and a substantiated expectation of causality between the law and the aims.[16]

[16] Operationalization is the process of redefining an ambiguous concept to make it measurable in order to perform empirical observations.

This thesis recommends to operationalize aims that are in essence measurable. For instance, the *perception* of personal data control by European citizens can be measured. Another option is to use a proxy.[17] The amount of personal data security breaches serves as a proxy for the aim of personal data control. Fundamental rights that are associated with the aims of the legislation, such as the freedom of speech and the freedom of expression, have an intrinsic value, which cannot be operationalized. These important non measurable aims should be included separately as informative input for a democratic legislative decision making process. An effective consideration of the democratic decision making process necessitates an extensive overview of potential negative effects as well.

To provide a reasonable expectation of effectiveness, an extensive study of the expected effects is recommended by means of academic literature, secondary available comparative (quantitative) analysis and expert interviews.[18] This threefold approach, adhered in this thesis, has enhanced the knowledge about expected effects and requires further development and a wider application.[19] As a result, a conceptual framework clarifies the effects to enhance the decision maker's information.[20]

Before the introduction of the law, the increased information about expected positive and negative effects and non-measurable aims allows for a more enhanced discussion about the desirability of the legislation. Ideally, the expected effects of the measurable part of the legislation will be quantified in order to clarify and structure the discussion about the desirability of the law. Consequently, the discussion solely concerns normative choices about the balance between non quantifiable effects with the sum of the measurable positive effects and negative effects. After the introduction of the law, the central registration of breach notifications, surveys about the perception of the effectiveness of the law and the registration of relevant proxies are key tools to empirically measure effectiveness.

[17] A proxy is a measurable unit that can be used to represent a non-measurable unit, to approximate or substitute the current aims.

[18] Such as performed in this thesis in part ß.

[19] Currently, the fuzziness of the aims and the complexity of measuring effects hamper the determination of a reasonable expectation of causality between the measure and the aims pursued.

[20] See section 8.1.2 of this research for a conceptual diagram of the first order effect of SBNLs.

Table of Contents

Acknowledgements

This thesis has been conducted simultaneously for the master European Law at the University of Utrecht and the master Systems Engineering, Policy Analysis and Management at the Technical University of Delft. I have been studying for almost six years at these universities. Hence, the challenge to write a thesis on the interface of these two scientific domains emerged. Although I am used to simultaneously study in Utrecht and Delft, the aim to integrate these disciplines in one single thesis has resulted in an adventurous multidisciplinary project.

Many people assisted me in writing this thesis by their inspiration, support and confidence. Unfortunately, it is impossible to acknowledge them all, but nevertheless I would like to mention the following persons.

First and foremost, I sincerely appreciate the ongoing support for this uncommon project of my supervisors, Sybe de Vries, Bauke Steenhuisen, Prof. Michel van Eeten and Jan van den Berg. Furthermore, advice given by statistical experts in the empirical part β has helped me tremendously. Shirin Tabatabaie and Hadi Asghari, both PhD candidates at the TU-Delft, introduced me in the 'POLG approach' of methods and techniques to statistically analyze the regulation of cybersecurity. Also, I would like to offer my special thanks to Fabio Bisogni, also a TU-Delft PhD candidate. He offered me vital assistance in constructing the independent variables and rethinking the quantitative analysis. An interview with Thijs Urlings, Assistant Professor at the TU-Delft and discussions with Catherine Endtz, graduate student Economics, and Bram Eidhof, PhD candidate at the University of Amsterdam, provided essential additional knowledge about the fixed effects regression method. Apart from this, I want to thank all the experts interviewed in the context of this thesis for their valuable input (listed in the bibliography). Furthermore, I wish to acknowledge the help provided by Christof Abspoel, Kees Cath, Robert van Mastrigt, Frank Nieuwesteeg and Timo Vosse, for their assistance in dotting the i's and crossing the t's. Finally I would like to thank friends and family for their enduring support.

Bernold Nieuwesteeg

August 2013

List of tables

List of figures

List of acronyms and abbreviations

ECHR	European Convention on Human Rights
AFSJ	Area of Freedom, Security and Justice
CAS	Complex Adaptive System
CERT	Computer Emergence Response Team
Charter	Charter of Fundamental Rights of the European Union
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
CWII	Cyber warfare infrastructure
CWP	Commission Work Program
ECHR	European Convention on Human Rights
ECP	European Cybercrime Policy
EFMS	European Form for Member States
ENISA	European Network and Information Security Agency
EP3	European Public-Private Partnership for Resilience
FDIS	Framework Decision on attacks against information systems
NCSC	National Cyber Security Centre
NIS	Network and Information Security
PCD	Proposed Cybersecurity Directive
PDIS	Proposed Directive on attacks against information systems
PDPR	Proposed Data Protection Regulation
PJCC	Police and Judicial Co-operation in Criminal Matters
SBNL	Security breach notification law
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union

Preface: law and its impact on society

Legal research often describes and prescribes the closed system of laws and its underlying legal values. For example, whether these legal values are guaranteed or whether normative goals are properly balanced. Typical legal research questions such as 'to what extent do fundamental freedom laws conflict with fundamental rights?', 'how may competition law differ among several justice systems?' or 'in what line did the concept of mutual recognition develop and how should develop further?' reflect this approach. These questions preeminently review the law from within the closed system of laws.

Though the questions above do imply societal relevance, they hardly inspire empirical studies of the law and its impact on society. Impact on society such as the enhancement of cybersecurity by means of security breach notification laws can be regarded as an external question. This concerns an assessment whether a rule attains the goals it aims to attain. I regard this as the opposite of internal questions that assess the law itself, mentioned above.

Legal research does tend to ask questions about impact but often measures impact on law instead of impact on society. Impact on law for instance concerns the correct and timely transposition of Directives.[21] This is an internal question. A European Directive is considered to have a large (legal) impact if it is transposed correctly into national law.[22]

Impact on society is harder to measure than the impact on law. Whereas impact on law may, for instance, be measured by the number of correct and timely transposed Directives, measuring impact on society requires extra efforts and can vary in complexity. Impact on society is fairly attainable if the law prescribes a certain level of protection. The environmental impact assessment of the maximum NO_x emission levels of cars that are prescribed by European law for instance is attainable because NO_x values are clearly measurable and there is a clear relation between NO_x values and the health of citizens.[23] Complexity increases if a law aims to interfere in the complex world of cybersecurity. Security breach notification laws are such laws.

[21] For example, see: Bernard Steunenberg and Wim Voermans, 'The transposition of EC Directives: A comparative study of instruments, techniques and processes in six Member States' (*WODC*, 2006) <https://openaccess.leidenuniv.nl/bitstream/handle/1887/4933/5_360_361.pdf?sequence=1> accessed 11 June 2013 & Dionyssis G. Dimitrakopoulos, 'The transposition of EU law: Post-decisional politics and institutional autonomy' (2001) 7(4) *European Law Journal* 442-458.

[22] This is called an impact assessment *ex post*, because the effect of a law is measured after its introduction.

[23] For example: Council Directive (EC) 96/96 on the approximation of the laws of the Member States relating to roadworthiness tests for motor vehicles and their trailers [1996] OJ L49.

Thus, legal research often internally describes and prescribes the system. What legal researchers call empirical impact assessments often measure impact on law instead of impact on society. If impact on society is assessed, it is often performed to demonstrate fairly simple causal relationship. Assessing impact on society of laws can be more complex. To understand more about this complexity, legal impact assessments could benefit from a multidisciplinary perspective as demonstrated in this thesis. A multidisciplinary perspective can take different relationships into account that are the building block for a more complex effect of the law.

Impact assessments on society could potentially greatly enhance the effectiveness of laws. In general, there is a substantial degree of consensus among policy analysts about the importance of impact assessment as a key tool to ensure the viability of proposed pieces of legislation.[24] Studies stress the need for the availability of data that help perform these analyses.[25]

The theme of this thesis is cybersecurity from a European law and security economics perspective. The security breach notification law is highlighted. New Internet laws, such as security breach notification laws, in particular require state-of-the-art insights in societal impact. The Internet is changing rapidly, there is uncertainty on the effects of laws and there are many new simultaneous legislative initiatives. Therefore this contributes an empirical perspective on the legal effects of security breach notification laws.

Given the aforementioned, the thesis has two normative starting points relating to the impact of law on society. The first normative starting point is that legislation can be valued by empirical measurement, and that measuring impact on society is relevant for the quality of the legal system. As the nexus between the law and the question relating to effectiveness becomes stronger, the law is less symbolic and more instrumental. The second normative starting point is that legislation can be necessary to mitigate societal problems if the total sum of benefits is higher than the total costs on society.[26] Internet insecurity is to a great extend a problem of cybersecurity economics and security breach notification laws are proposed by the European legislature to interfere in this domain. This thesis analyses the legal position and societal effects of security breach notification laws.

[24] Andrea Renda, *Impact Assessment in the EU, The State of the Art and the Art of the State* (CEPS Paperbacks 2006) 133.

[25] For instance, see the recommendations in: Ross Anderson, Rainer Böhme, Richard Clayton & Tyler Moore, 'Security Economics and the Internal Market' (*ENISA*, 31 January 2008) <http://www.enisa.europa.eu/ publications/archive/economics-sec>, Accessed 10 December 2012.

[26] However, some societal costs, such as insufficient fundamental rights protection, are hard to quantify and require a minimum level of protection.

1 Introduction

This thesis scrutinizes the proportionality and describes the subsidiarity of proposals for security breach notification laws (hereafter: SBNLs) in the European Union.

A security breach notification law is an obligation for governments and companies to notify security breaches to the person whose data is breached and/or a supervisory authority. A *security breach* is defined by a loss of data and/or a (significant) loss of integrity of computer systems. If a company does not comply with the law, a penalty can be imposed.

A law is proportional if the requirements of effectiveness and necessity are met.[27] Effectiveness means that there is a causal relationship between the measure and the aim pursued. Necessity means that no less restrictive policy options are available that achieve the same aims.[28] The closely linked subsidiarity test assesses the necessity of the *European Union* approach: the question whether the aims of the SBNL and cybersecurity cannot be achieved sufficiently by the Member States individually.[29] Subsidiarity is described more limited because this is to a great extent a political question.

Why these tests? Subsidiarity, laid down in Article 5(3) TEU, and proportionality, laid down in Article 5(4) TEU, are fundamental principles of EU law. They demand the European legislature to not go beyond what is necessary to attain the objectives in the Treaties and to only adopt measures if a European Union approach has added value.

The laws that have been tested are Article 31 of the proposed Data Protection Regulation (Hereafter: PDPR) and Article 14 of the proposed Cybersecurity Directive (Hereafter: PCD). Article 31 PDPR concerns a single uniform *personal data breach* notification. Article 14 PCD concerns the harmonization of national (significant) *loss of integrity* breach notification obligations. The Netherlands recently initiated a legislative

- A personal data breach entails the unauthorized access to and/or theft of personal data.
- A loss of integrity entails the loss of control over computer systems, i.e. the loss of confidentiality, integrity or availability of the computer system.
- A personal data breach always entails a loss of integrity, but a loss of integrity can also occur without the loss of personal data.

[27] *Volker Schecke* (n 1).

[28] Chalmers (n 2) 362. There is also a third criterion, proportionality strictu sensu, which is sometimes mentioned separately, see section 3.2.1 of this research.

[29] See also Protocol (No 2) on the Application of the Principles of Subsidiarity and Proportionality [2007] OJ C-310/207; Graig and de Búrca (n 3) 95.

process for such a loss of integrity breach SBNL. This initiative is an example of a national SBNL, which Article 14 PCD aims to harmonize.

The aim of the proposed SBNLs is a central element of this thesis, because the suitability of the legislation to achieve this aim is part of the proportionality test. The aim of the PDPR is "to ensure that individuals are in control of their personal data and trust the digital environment"[30] in order "to increase the effectiveness of the fundamental right to data protection".[31] The aim of the SBNL in the PCD is: "to create a culture of risk management and improve the sharing of information between the private and public sectors."[32]

The thesis consists of three parts. Part α is a theoretical study from a legal perspective. Part β is an empirical study from a security economics perspective. Hence, this thesis is multidisciplinary. Part γ contains the synthesis and conclusions of part α and part β. This has the implications that some concepts are explained a bit more in depth than usual to make the entire thesis to a great extent understandable for scholars of both disciplines.

In part α, first, the European cybersecurity legal and policy framework is highlighted. It is analyzed to what extend cybersecurity is anchored in the Treaties, Charter and soft law, in order to answer the question whether the European approach regarding cybersecurity is necessary. Second, the European proposals are introduced in relation to American laws. Third, the principles of subsidiarity and proportionality are assessed in the light of SBNLs.

Part β builds on insights about the structure of the SBNLs in part α by empirically analyzing the (complexity of) effects of SBNLs on society. This is indispensable to substantiate the first element of the legal proportionality test. To structure the empirical study, a first and second order effect of SBNLs is distinguished. The first order effect is the effect of (characteristics of) SBNLs on the amount of breach notifications. Generating notifications is not one of the aims of the proposed legislation, but a means to achieve the second order effect. The second order effect is the effect of the law on society. A literature review is conducted to provide an overview of what is already known concerning those two effects. The quantitative analysis systematically assesses the first order effect of American SBNLs by a longitudinal dataset containing security breach notifications. The qualitative analysis reviews the perception of first and second order effects of by means of Dutch expert interviews. It is also used as a review for the quality of the quantitative analysis. The demarcation of the research in part β is displayed in figure 1.

[30] *Impact assessment PDPR* (n 6), section 5.3.1.
[31] Ibid.
[32] *Impact assessment PCD* (n 8), section 6.1.

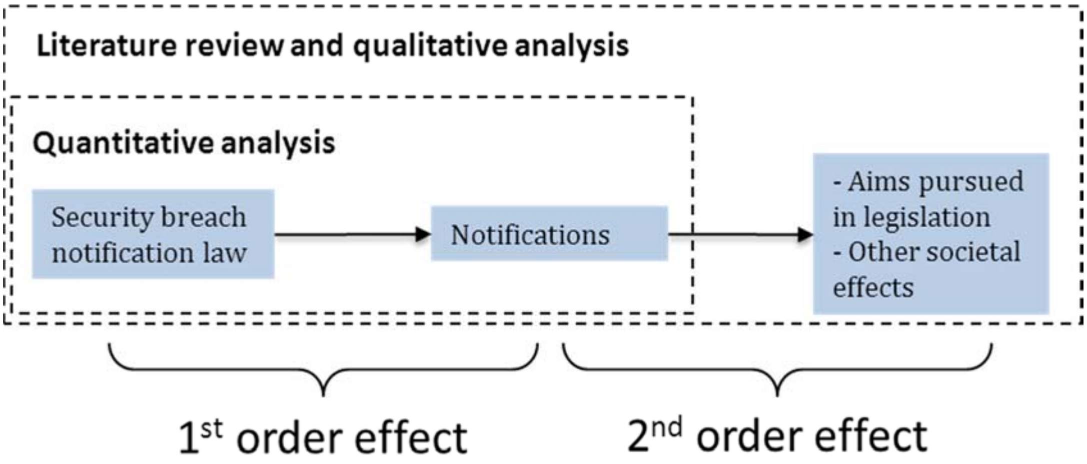

Literature review and qualitative analysis
Quantitative analysis
Security breach notification law
Notifications
- Aims pursued in legislation
- Other societal effects
1st order effect
2nd order effect

Figure 1: the demarcation of the research in part β

Hence, the question whether European legislation on SBNLs is necessary and proportional is answered in part γ by substantiating the legal subsidiarity and proportionality test of part α with the empirical analysis of effects in part β.

This introduction sketches the context of the research subject, namely the Internet, with specific attention for Internet security. Within the subject of Internet security, Internet insecurity problems are analyzed from a security economics perspective. Hereafter, the SBNL and the concepts of subsidiarity and proportionality are introduced. After this, research objectives and questions are presented. Finally, the thesis' approach is outlined.

1.1 Internet and security

The Internet is important and special. The World Wide Web is an impetus for economic growth and non-economic values such as the freedom of speech. Internet insecurity is a threat for the development of and activities on the Internet. The problem of cybersecurity economics precludes an easy solution to mitigate Internet insecurity. Increased Internet insecurity has triggered governments to adopt SBNLs.

1.1.1 The Internet: an impetus for economic growth & non-economic values

The Internet rapidly emerged from a university network to one of the most important infrastructures for the world economy. While at the end of 2000, merely 360 million people used the Internet, approximately 2.4 billion people used the Internet on a regular basis by mid-2012.[33] A McKinsey report estimated that the Internet accounts for 21% GDP growth in developed economies between 2006 and 2011.[34] The Internet is a catalyst for mature economies to maintain their welfare level when coping with aging populations and slowed productivity growth. Hence, there are significant consequences

[33] 'Internet statistics'. <www.Internetworldstats.com> accessed 14 April 2013.

[34] Matthieu Pélissié du Rausas et al, 'Internet Matters: The Net's sweeping impact on growth, jobs and prosperity'. (*McKinsey Global Institute*, May 2011), 2 <http://www.mckinsey.com/insights/high_tech_telecoms_Internet/Internet_matters> accessed 27 December 2012.

if the Internet as an infrastructure hampers, which is the case if personal data is lost or stolen or if (public services) such as Internet banking are unavailable. This could result in a loss of economic activity and a loss of trust in the economy.

In addition, the Internet is a special infrastructure and is a conductor for non-economic public values. Already in 1996, at the dawn of a global Internet economy, John Perry Barlow declared 'the global social space we are building to be naturally independent', already hinting on these special characteristics.[35] Internet is indeed characterized by openness and transborderness.[36] The Internet cannot be controlled by one single stakeholder and there is no central governance structure, although some stakeholders govern parts of the network and thus have stronger influence than others.[37] The Internet and its equal information exchange are accessible for many. The Internet therefore is a unique platform for conducting non-economic values such as public speech and the freedom of expression. However, Internet insecurity may also emerge if the information exchange over the Internet increases. The security of information on the Internet, called 'cybersecurity' in this thesis, is usually defined as:

> "the protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. Information security includes those measures necessary to detect, document and counter such treats"[38]

Cybersecurity thus concerns the confidentiality, integrity and availability of (personal) information.[39]

Concluding, the Internet is an important and special infrastructure for stimulating the economy as well as a platform for expressing non-economic values. Internet security is important for the development of the Internet.

[35] John Perry Barlow, 'Declaration of Internet independence' (*eff.*org, 9 Februari 1996) <http://w2.eff.org/Censorship/Internet_censorship_bills/barlow_0296.declaration.> accessed 9 January 2013.

[36] At the same time the nature of the Internet is changing, from an open interoperable and unified system, towards a closed system with fewer stakeholders, see: Jonah Force Hill 'Internet Fragmentation: Highlighting the Major Technical, Governance and Diplomatic Challenges for U.S. Policy Makers' (Paper, Harvard Kennedy School 2012).

[37] For example the Internet Corporation for Assigned Names and Numbers (ICANN) performs a number of important Internet related tasks such as the distribution of top level domain names (TLDs). <www.icann.org> accessed 11 June 2013.

[38] Karl de Leeuw 'Introduction', in Karl de Leeuw & Jan Bergstra (eds.), *The History of Information Security: A Comprehensive Handbook* (Elsevier, 2007) 2-3.

[39] Axel Arnbak and Nico van Eijk 'Certificate Authority Collapse, Regulating Systemic Vulnerabilities in the HTTPS Value Chain' (2012) TRPC, 20. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2031409 > accessed 8 January 2012.

1.1.2 Security breaches: a personal data breach and loss of integrity

Internet insecurity can harm both economic and non-economic goals of the Internet. The Internet has rapidly become more insecure through increased criminal activity, caused by the increase of Internet users and economic activity on the Internet. Crime follows opportunity as the fundamental principle of criminology says.[40] This thesis distinguishes the loss of data and the loss of integrity as two concepts that both can entail a security breach. A personal data breach means that third parties access or use personal data illegally. A loss of integrity of information system means that a serious attack causes damaged and breached computer systems, resulting in unavailable services and a loss of control. A loss of integrity has a broader scope than a personal data breach. A personal data breach always involves loss of integrity because if personal data is lost a defense system is breached, but a loss of integrity does not necessarily involve a personal data breach. For example, in March 2013, a series of cyberattacks (DDOS) on Dutch banks did not result in a loss of data but in the unavailability of mobile banking services. Most (banking) computer systems have a multiple layers of defense and only a breach of the last defense layer results in actual loss of data.[41] Another example is the fact that criminals possibly want control over certain aspects of computer systems that do not store personal data. For instance, Dutch water utilities have separated computer systems for the operation of their water processes and their customers.[42]

There are many tools for criminals to execute a security breach. A few examples of tools and actions relevant for organizations are: the disruption of computers by malicious software (malware), Distributed Denial of Service (DDoS) attacks with botnets (networks of compromised computers) and identity theft by phishing. Some tools, such as DDoS attacks, are more suitable for disrupting computer systems and are more likely to cause a loss of integrity without a loss of personal data. Other tools, such as banking Trojans (a type of malware) focus more on personal data theft for economic purposes, such as banking fraud. The tools to perform a security breach will not be discussed in depth.[43] For the purpose of this thesis, it is sufficient to make the distinction between loss of integrity and loss of personal data.

[40] Paul Hunton, 'The growing phenomenon of crime and the Internet: A cybercrime execution and analysis model' (2009) 25 *Computer Law & Security Review* 528, 529.

[41] Interview with Ronald Prins, Director, Fox IT (Delft, the Netherlands, 12 April 2013).

[42] For instance, Dutch water utilities have separated computer systems for the operation of their water processes and their customers. Only the latter system contains personal data. (Interview with Rogier Ragetlie, Security Manager, Brabant Water ('s Hertogenbosch, the Netherlands, 25 April 2013).

[43] For further reading, Hadi Asghari has listed extensive list of online security threats faced by end users, see: Hadi Asghari 'Botnet Mitigation and the Role of ISPs' (Master Thesis, Delft, University of Technology) 7-12; 'Cyber Security Report 2012' (*National Cyber Security Centre,* 19 September 2012), 22-34 < https://www.ncsc.nl/english/current-topics/news/ncsc-publishes-cyber-security-report-2012.html> accessed 11 June 2013.

1.1.3 An increase of security breaches and social costs

Cybercrime is perceived as a threat and is a part of daily life.[44] Most Internet users in Europe 'have seen or heard something about cybercrime in the last 12 months'.[45] A 2010 U.K. survey under 964 IT and business managers from 15 industry sectors stated that 88% of the respondents experienced a data breach in his or her company.[46]

The costs of cybercrime are hard to estimate, but probably have increased significantly over the last few years. Dutch banking fraud damage indicates this upward trend. In 2011, this damage was projected at 35 million euro, a tripling with respect to 2010.[47] In the first half of 2012, the damage of Internet crime was 27.3 million euro, which confirms the upward trend.

The estimation of the cost of cybercrime can depend on the interest of the stakeholder. Internet security companies for instance could have an interest in an exaggeration of the costs to sell more products.[48] In the United Kingdom the costs of Internet crime for companies are estimated at 5.9 million dollar per year and average annual costs per capita in are estimated 98 dollar according to Internet security companies.[49] The total annual worldwide Internet crime costs are estimated to exceed 100 billion dollar.[50]

The cost of cybercrime can be divided in the direct costs and indirect costs. According to a recent scientific study, the direct annual costs of cybercrime, the damages of a cyberattack, "might amount to a couple of dollars per [UK] citizen per year".[51] Indirect costs and defense costs are at least ten times of the direct costs.[52] Hence, the protection of citizens against cybercrime is more costly then the direct financial impact of the crime itself.

[44] For more analysis, see the following factsheet about cybercrime 'Eurobarometer 390 for the Netherlands' (*European Commission*, 2012) <http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_fact_nl_en.pdf> accessed 7 January 2012.

[45] 'Eurobarometer 390' (*European Commission*, 2012), 61 <http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf> accessed 7 January 2012.

[46] '2010 Annual Study: U.S. Enterprise Encryption Trends' (*Ponemon Insitute,* November 2010), 5 < http://www.symantec.com/content/en/us/about/media/pdfs/Symc_Ponemon_Encryption_Trends_report_Nov2010.pdf> accessed 15 July 2013.

[47] 'Cybersecurity Assessment Netherlands'. (*National Cyber Security Centre*, 19 September 2012). <https://www.ncsc.nl/english/current-topics/news/ncsc-publishes-cyber-security-report-2012.html> accessed 21 April 2013; 'Fraude report Internet banking and skimming' (*Nederlandse Vereniging van Banken*, 2012). <http://www.veiligbankieren.nl/nl/nieuws/fraude-Internetbankieren-stijgt-eerste-half-jaar-met-14_.html> accessed 11 June 2013.

[48] Ross Anderson, Chris Barton, Rainer Bohme, Richard Clayton, Michel van Eeten, Michael Levi, Tyler Moore, Stefan Savage, 'Measuring the Cost of Cybercrime' (2012) Workshop on Economics of Information Security 6/2012 <http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf> accessed 7 January 2013.

[49] '2011 Cost of Cyber Crime Study' (*Ponemon Institute*, August 2011) <http://www.hpenterprisesecurity.com/collateral/report/2011_Cost_of_Cyber_Crime_Study_August.pdf> accessed 30 November 2012.

[50] 'Press release on Symantec Security Report' (Symantec, 7 September 2011) <www.symantec.com/about/news/release/article.jsp?prid=20110907_02> accessed 28 November 2012.

[51] Anderson (n 48) 25.

[52] Ibid.

1.1.4 The problem of cybersecurity economics

The Internet is increasingly important for our economic and social life. As a result, the Internet is becoming increasingly insecure as crime follows opportunity. In addition to that, there is a problem of cybersecurity economics.

The problem of cybersecurity economics is characterized by:

- Imperfect information about effective security measures because of the complexity of big data and defense systems.
- Negative externalities on society concerning the costs of security breaches.
- Underpowered incentives to invest in security, protect consumers information and share knowledge with competitors.

The Economist stated in 2010:

> 'The world contains an unimaginably vast amount of digital information which is getting ever vaster ever more rapidly'[53]

Digital information includes personal data of customers and confidential information of companies. Hence, it is a vulnerable asset. Breaches of defense systems and theft of this personal information harms society. Ideally, companies would take proper measures to prevent data and security systems to be breached. But, 'big data' of companies is very complex and extensive which makes it extremely difficult to oversee and defend.

Moreover, companies have incentives for suboptimal investment in security. That is caused by the fact that companies do not bear the full costs of a security breach.[54] For example: a hack on the control systems of an energy production company can result in a power failure of a day.[55] Such a company would incur for instance a 1 million cost from lost income and damage, while the indirect costs of companies that are not able to operate their businesses are the multiple of that. Of course, companies can claim for damages. However, such a claim would probably be rejected on the grounds of a force majeure situation, an extraordinary event beyond the control of a company which prevents the party from fulfilling its obligations.[56]

Apart from this, there are little incentives for companies to invest in security because consumers do not want to pay for it. Internet security is a so called 'market for lemons'.

[53] 'Data, Data everywhere' (*The Economist,* 25 February 2010). <www.economist.com/node/15557443> accessed 11 June 2013.
[54] Deirdre Mulligan, 'Security Breach Notification Laws: Views from Chief Security Officers' (*University of Berkeley School of Law*, December 2007), 13 <http://www.law.berkeley.edu/files/cso_study.pdf> accessed 11 June 2013.
[55] For comparison: 'Waterinstallatie beschadigd bij cyberaanval' <www.automatiseringgids.nl/nieuws/2011/47/waterinstallatie-beschadigd-bij-cyberaanval> accessed 11 June 2013.
[56] A definition of 'Force Majeur' can be found at <www.trans-lex.org/944000> accessed 21 April 2013.

The majority of consumers are not able to distinguish a good secured company from a bad secured company, because they have no information to value security practices.[57] A company thus cannot invest in security to gain competitive advantage and in fact incurs more costs compared to companies how invest less in security.

Besides, there are less direct incentives to protect consumer information. Trade secrets and other competitively sensitive information are vital for the operation of business, but consumer information often is not.[58] The incentive to protect security best practices for competitive reasons results in reluctance to share security knowledge and best practices with competitors in order to achieve concerted practices concerning security. For example, Dutch banks only recently initiated a structured information exchange about DDoS attacks.[59] If the security breach is fixed internally the impact at company level is limited, but if other actors are unaware of this security threat and cannot improve their own defense systems, negative effects for society emerge.

Additionally, companies do not have incentives to notify consumers, because this would damage their reputation and possible results in claims for damages. Moreover, this has the effect that consumers do not have incentives to improve their own behavior related to security, because they are not aware of insecure situations that occurred.

1.1.5 Governments triggered to adopt security breach notification laws

Internet insecurity has triggered the European Union to propose SBNLs.[60] The increased level and significance of personal data losses stimulated the Commission to propose a personal data SBNL in Article 31 of the PDPR.[61] The increase of the frequency and severity of network and information security incidents has been a main reason for the Commission to propose a loss of integrity SBNL in Article 14 PCD.[62] The concept of the SBNL is borrowed from the United States. The initiation of the two European proposals for SBNLs forms a part of the development of a European legal framework concerning cybersecurity. The cybersecurity framework is extensively discussed in chapter 2 and the origins of SBNLs in chapter 3.

[57] Ross Anderson, 'Why Information Security is Hard – An Economic Perspective (*University of Cambridge*, December 2001) <http://www.cl.cam.ac.uk/~rja14/Papers/econ.pdf> accessed 25 June 2013.

[58] Mulligan (n 54) 13.

[59] 'Banken beloven informatie over cyberaanvallen onderling te gaan delen' (*Tweakers*, 15 April 2013) <http://tweakers.net/nieuws/88507/banken-beloven-informatie-over-cyberaanvallen-onderling-te-gaan-delen.html> accessed 13 June 2013.

[60] Anderson (n 25); Researches in the field of security economics have recommended policy options for governments, see: Tyler Moore, 'The economics of cybersecurity: Principles and policy options' (2010) 3(3-4) *International Journal of Critical Infrastructure Protection* 103.

[61] Paul de Hert and Vagelis Papakonstantiou 'The proposed Data Protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals' (2012) 28(3) *Computer Law and Security Review* 130, 140.

[62] *PCD* (n 4), 2.

The United States, the European Union[63] [64] and the Netherlands[65] all have (pending) initiatives on SBNLs:

- The United States started to adopt personal data SBNLs at the beginning of this century. California was the first state to adopt legislation in 2002 and other states quickly followed. In 2006, 27 states adopted legislation and 16 states had pending legislation. In 2012, 46 states adopted an SBNL.
- In 2012, the European Commission proposed the Data Protection Regulation that contains a general security breach notification law for personal data. In 2013, the Commission proposed a Cybersecurity Directive that aims to harmonize national loss of integrity SBNLs.
- The Netherlands initiated a national loss of integrity SBNL. In mid-2013, the structure of the final legislation is being sketched by means of consultation rounds.

An obvious first order aim of the SBNL is to generate security breach notifications.[66] The second order aim of the PDPR is "to ensure that individuals are in control of their personal data and trust the digital environment"[67] in order to "to increase the effectiveness of the fundamental right to data protection".[68] The second order aim of the SBNL in the PCD is: "to create a culture of risk management and improve the sharing of information between the private and public sectors."[69]

1.2 Research objectives

This thesis focuses on two fundamental principles of European law: subsidiarity and proportionality. To recall:

- Subsidiarity (Article 5(3) TEU) concerns the question whether a European Union approach is necessary, thus whether the aims of the SBNL cannot be achieved sufficiently by the Member States individually.
- Proportionality (Article 5(4) TEU) concerns:
  - 1.) an effective measure: the measure suitable to achieve the aim pursued
  - 2.) a necessary measure, in the sense that no less restrictive alternative measures are available.

This thesis provides to enhance the proportionality analysis of the European Commission and rethink measuring impact on society.

[63] *PDPR* (n 4)
[64] *PCD* (n 4). In 2009, the European Union had already adopted two Directives for both a loss of integrity and a personal data SBNL for telecommunication providers.
[65] Interview with David van Duren & Bob Rijkhoek, Policy Analysts, Ministry of Safety and Justice. (The Hague, the Netherland, 6 November 2012).
[66] Literally mentioned *Impact assessment PCD* (n 8), Annex 13.
[67] *Impact assessment PDPR* (n 6), section 5.3.1.
[68] Ibid.
[69] *Impact assessment PCD* (n 8), section 6.1.

The European Commission has tested proportionality only marginally in its impact assessment of both the PDPR and the PCD. The Commission does not substantiate how the SBNLs will achieve the aims pursued.[70] This is a deficiency in the analysis of this proposed legislation. The Commission did not mention in what way the SBNL is suitable to achieve the aim "to ensure that individuals are in control of their personal data and thrust in the digital environment" and "to create a culture of risk management and improvement of information sharing between private and public parties". Given the fact that there are no arguments about whether the proposals are suitable to achieve the aims pursued, there is a societal risk for an ineffective law that imposes significant administrative burdens on companies and costs on society.

Legal scholars, the European legislators and the Court, usually assess the first aspect of proportionality limitedly. In legal research, the first aspect of the proportionality test is regarded to "rarely cause problems" and is "the least problematic".[71] The European Commission does not seem to substantiate causality very well, as the PDPR and PCD indicate. The Court is regarded to be able "perfectly well to assess the causal relationship between the measure and their objectives".[72] However, insufficient substantial input on the complexity of the effects can hamper this assessment, as this thesis will show. Instead of focusing on the first aspect of proportionality, the debate in legal research concentrates on the second aspect; the balance that needs to be struck between several (fundamental) rights.

This thesis challenges the aforementioned assumption that determination of causality is straightforward. This is done by a more substantive assessment of the proportionality test. This can increase knowledge about the effects of the law. The Commission did not provide information that gives a reasonable expectation of causality between the measure and the objectives to be attained. This knowledge gap concerns amongst others, which characteristics of an SBNL give incentives for compliance, whether individuals will get more in control of their data and whether the law benefits information sharing and Internet security. Moreover, the desirability and validity of the aims of legislation is unknown. Will the law be effective from a societal perspective if the aims pursued are achieved altogether? An empirical analysis can enhance understanding about the effects of SBNLs.

Therefore the goal of this research is to more substantively measure effects empirically to enhance the knowledge about these effects in order to improve the important legal proportionality test. The problem will be analyzed from security economics perspective, because "an economic perspective has yielded invaluable insights into the analysis and

[70] Neither in both the proposed text and impact assessment of the PDPR and the PCD.

[71] Jans (n) 240, 245, this paper concerned the proportionality test regarding measures of Member States, but the same limited attention applies to measures of the European Union. The marginal test of proportionality of the European Commission in both the PDPR and the PCD stresses this.

[72] Jans (n) 245.

design of information security mechanisms."[73] The effects of the laws proposed cannot be measured directly, as they are not yet adopted. However, literature review and quantitative analysis on the effects of American SBNLs and the perception of the law by means of qualitative analysis can provide a forecast of the effects of the proposed laws.

The second element of the proportionality test assesses the necessity of the two European proposals. The European legislature must always choose for the least restrictive measure available. The SBNL can restrict companies, because it infringes the fundamental freedom to conduct business by imposing administrative, compliance- and reputational costs.[74] Possibly, another approach imposes fewer burdens on companies while attaining the same objectives.

The principle of subsidiarity is closely linked with proportionality and will be discussed as well, although more limited. The necessity of a European Union approach is partly a political question, because national parliaments determine the limits of European Union action to a great extent.[75] This fundamental question of European Law appropriateness as such falls beyond the scope of this thesis. Instead, the arguments for a European Union approach regarding cybersecurity and in special SBNLs brought forward by the European Commission are displayed. In addition to this, insights regarding subsidiarity from the comparative analysis of U.S. SBNLs are added to this view.

This research aims to scrutinize the proportionality of Article 31 PDPR and Article 14 PCD and discuss arguments for the necessity of a European cybersecurity approach.

α.) an analysis of the cybersecurity framework and European proposals for SBNLs from a European law perspective

β.) an analysis of the effects of an SBNL empirically from a security economics perspective, by means of literature review, quantitative and qualitative analysis.

1.3 Research questions

The main research question of this thesis is formulated as follows:

To what extent does the current European Union approach concerning general SBNLs stand the test of proportionality?

The main question is divided into several sub questions.

[73] Tyler Moore and Ross Anderson, 'Internet Security' in Martin Peitz & Joel Waldfogel (Eds.), 'The Oxford Handbook of the Digital Economy' (Oxford University Press 2011) 584.

[74] *Scarlet Extended* (n 12). The freedom to conduct business can be infringed by imposing unnecessary administrative burdens on companies.

[75] Chalmers (n 2) 129; in some areas, the European Union has an exclusive competence, and the subsidiarity question is less relevant, but cybersecurity is no such area, see Article 3 TFEU.

Part α: what is the legal position of an SBNL in relation to the European Cybersecurity Framework?[76]

Chapter 2:

- What are the main goals and policies of the European cybersecurity policy framework?
- What are the main legal bases for European cybersecurity laws?
- How are the PDPR and the PCD related to these legal bases?

Chapter 3:

- What are the origins of SBNLs in the United States, the European Union and the Netherlands?
- What is the opinion of the European legislator on subsidiarity and proportionality of the European SBNLs?
- Which design parameters can be distinguished based on the two legislative initiatives?

Part β: what are effects of security breach notification laws?

Chapter 4:

- What effects of SBNLs can be found in literature?

Chapter 5 & chapter 6:

- What is the relation between design parameters of U.S. SBNLs and the amount of breaches?

Chapter 7:

- What effects do security experts and managers expect?
- How do they reflect on effects found in literature and quantitative analysis?

Part γ: synthesis and conclusions.

Chapter 8

- What is the relation between the effects found and the aims of the legislation?

1.4 Research methods

This research is conducted by literature research, quantitative and qualitative analysis.

1.4.1 Literature research

The legal research in part α is for the most part literature research. This is done by reviewing various legal sources, such as scientific articles, policy documents of the European Commission (communications, action plans and programs) and European

[76] Design parameters, treated in chapter 3, are aspects of functional characteristics of the law.

hard law (Directives and Regulations). The literature review in part β discusses first and second order effects of American SBNLs. For this purpose, authoritative scientific databases such as scopus, sciencedirect and ssrn are searched.[77] Frequently used keywords of this search are 'security breach notification law', 'identity theft', 'data breach notification law', 'disclosure laws' and 'Internet security'.

1.4.2 Quantitative analysis

A quantitative analysis is performed in part β in order to measure the relationship between the design parameters of SBNLs and the amount of notifications generated. In mid-2013, the PDPR and PCD are still proposed legislation. Obviously, it is impossible to empirically measure the effects of the proposed SBNLs.

Fortunately, the U.S. has already adopted SBNLs.[78] Therefore, an American database, which contains security breaches, is used for the purpose of this thesis.[79] The dataset concerns longitudinal data: data of multiple subjects (states) with multiple measurements in time (years). This longitudinal dataset allows an analysis of the effect of the adoption of the law on the amount of notifications in the database. Moreover, the effects of characteristics of the 46 American SBNLs that have been adopted can be researched. Those characteristics have been constructed by authoritative legal sources and review of the law.

The quantitative approach requires a careful interpretation of the statistical relationships.[80] This applies in particular to this quantitative analysis, that studies the effectiveness of legislation. Only a few characteristics of the law can be viewed in the light of the amount of notifications in the database. Thus, limited in-depth knowledge can be gained about the 'why?' and the 'how?' of the results. Moreover, the data concerned is not collected for the purpose of this thesis, which implicates that it extensive analysis must be paid to the validity of the data.[81] Apart from this, it is complex to determine causality between the law and its effects on society. The effect of the law cannot be isolated easily from the effect of numerous other variables, such as the role of ISPs, the attitude towards risk in a country and the number of Internet users.[82] This implicates that extra efforts must be put in controlling for side effects.[83]

The approach of the quantitative analysis is as follows, taking this complexity into account. First, a descriptive analysis and comparison of means and medians is executed

[77] <www.scopus.com>; <www.sciencedirect.com>; <www.ssrn.com>.

[78] See section 3.1.1 of this research.

[79] The database of the Privacy Breach Clearinghouse is extensively discussed in section 5.1 of this research.

[80] Ibid, 167.

[81] Piet Verschuren & Hans Doorewaard, '*Designing a research project*' (Second edition, Eleven International Publishing 2010), 198; which is done in section 5.1.

[82] Michel van Eeten, Johannes Bauer, Hadi Asghari, Shirin Tabatabaie, 'The Role of Internet Service Providers in Botnet Mitigation: an Empirical Analysis based on Spam Data' (2010) OECD STI Working Paper 2010/5 <http://search.oecd.org/officialdocuments/displaydocumentpdf/?cote=DSTI/DOC%282010%295&docLanguage=En> accessed 11 June 2013.

[83] See section 5.1.4 and 5.1.5 of this research.

to discover rough patterns in the data. Second, a more advanced fixed effects regression is performed to control for several variations in time and between states.

Descriptive analyses, the Independent Samples T-test and the non-parametric Mann-Whitney test, are used to distinguish rough patterns in the data. The descriptive analysis is used to examine the representativeness of the data on different levels. The statistical tests are used to determine whether the means and medians of the amount of breach notifications differ significantly for different characteristics of the law.

The more advanced fixed effects regression is used to control for variation between time and states, because those variations can significantly influence the dependent variable. The strength of the fixed effects model is that it allows to control for certain omitted variables.[84] The regression 'automatically' controls for differences between states, which are constant over time and for differences over time, which are constant over states. The following box displays a short explanation about basic mechanism of the fixed effects regression.[85]

The mechanism of the fixed effects regression

One could imagine that the amount of firms in a state determines the amount of notifications in a state. A normal regression, that omits the control variable *firms per state*, would indicate that large states have more effective laws, because large states generate more notifications. This is a false conclusion, because the variable *firms per state* is omitted from the analysis and the amount of notifications depends on the number of firms in a state.

The fixed effects regression measures the *changes* in the dependent variable from 2005 until 2012. A state with a large number of firms in 2012, such as Texas, already had a large number of firms in 2005. If there are no changes in the amount of notifications are observed, this means that the adoption of the law in 2009 (probably) did not have an effect. In fact, the fixed effects regression assumes that omitted variables remain constant over time, because than any changes of the amount of firms are not caused by the omitted variable. The same applies for variations over time, which are constant over states. The automatic control for these kinds of variables results in a more accurate model.

The longitudinal dataset is essential for a fixed effects regression, because it allows for the measurement of *changes* of the dependent variable because there are multiple points in time needed to measure the amount of notifications in a state. An analysis for measurements over time is not allowed within a standard OLS regression analysis because multiple measurements per subject (state) result in forbidden correlations

[84] See: Marno Verbeek, *A Guide to Modern Econometrics* (Fourth Edition, Wiley, 2012), chapter 10: if an omitted variable does not change over time, than any changes in the dependent variable can not be caused by the omitted variable.

[85] Jos W.R. Twisk, *Applied Multilevel Analysis* (Cambridge University Press, 2006), chapter 6.

within the dependent variable.[86] These correlations are allowed in fixed effects regression, because an assumption is made concerning the correlation between multiple measurements per subject.[87]

Fixed effects regression is regarded as a sophisticated statistical tool, which also needs complete data.[88] There is a risk of over-interpreting the results if the data is not very accurate. On the other hand, descriptive analysis and a comparison of means do not control for variations over time and state; they are more basic statistical tools. Therefore results of the two analyses will be in conjunction with each other.

1.4.3 Qualitative analysis

The qualitative analysis concerns both exploratory and official interviews. A complete list of the experts interviewed can be found in the bibliography. The exploratory interviews with cybersecurity experts were held at the start of the research. Based on these interviews, the thesis problem definition is constructed. The exploratory interviews are also performed to receive more substantive information about, amongst others, the way in which the European legislature thinks about impact on society and the mechanism of the fixed effects regression.

Hereafter, four semi-structured expert interviews with open-ended questions have been conducted to inquire the first and second order effects of SBNLs and to reflect on the quantitative analysis. The open-end character allows for input of respondents on aspects that are not asked. The semi-structured setting also allows deviation from the storyline to explore relevant aspects. The interviews cannot be used to measure effects directly, because there is a risk of strategic answering and in most cases, there is no real life experience with a general SBNL. Instead, only the perception of effects can be measured. Apart from asking for effects, the respondents also have been asked to reflect on the results of the quantitative analysis. They are asked to value the statistical results and the quality of the dataset. The whole interview template is displayed in appendix A.

[86] The amount of breaches in a state in 2007 in, for instance, California will probably be correlated with the amount of notifications in 2008, because they come from the same state, see: Howard Seltman, *Experimental Design and Analysis* (Published online, 2009), chapter 15. <http://www.stat.cmu.edu/~hseltman/309/Book/chapter15.pdf> accessed 11 June 2013.

[87] See section 6.2.1 of this research.

[88] Fixed effects can be distinguished from random effects. Interview with Thijs Urlings, Assistent Professor, Innovation and Public Sector Efficiency, Delft University of Technology (Delft, the Netherlands, 3 May 2013): "Fixed effects delivers a 'within estimator', which analyses the differences in time within a state. Random effects uses a combination of a 'within estimator' and a 'between estimator' (also observes differences between states.) The random effects method uses variations in the data more efficiently, but preference will be given to fixed effects if the research units are unique and of importance, for instance individual states. This is the case in the current analysis.

1.5 The approach

As already mentioned, this thesis consists of three parts. Part α is a theoretical study from a legal perspective. Part β is an empirical study from a security economics perspective. Part γ contains the synthesis and conclusions of part α and part β.

Part α is characterized by a converging approach. In chapter 2, the general concepts and developments of the European cybersecurity framework are analyzed. This is done from a policy perspective and a legal perspective. Hereafter, the discussion narrows down to Article 31 PDPR and Article 14 PCD in chapter 3. The origins, proportionality and design parameters of the laws are analyzed from a legal perspective. The design parameters of the law form substantive input for the empirical analysis in part β.

Part β is characterized by a threefold approach. The analysis of the effects of SBNLs from a security economics perspective is performed by three different research methods. First, analytical suggestions and empirical measurements about these effects are distinguished in literature. Second, an American dataset is used to analyze the effects of (characteristics) of the law on the amount of notifications. Third, a quantitative analysis is performed review the perception of Dutch security experts and managers on effects of SBNLs and the outcomes of the quantitative analysis.

In part γ, the results of the three types of analysis are synthesized. This results in a conceptual framework and a comparison of the effects with the aims of the legislation, analyzed in part α. Hereafter, the conclusions and recommendations of the research are presented. The approach is displayed in the figure on the next page.

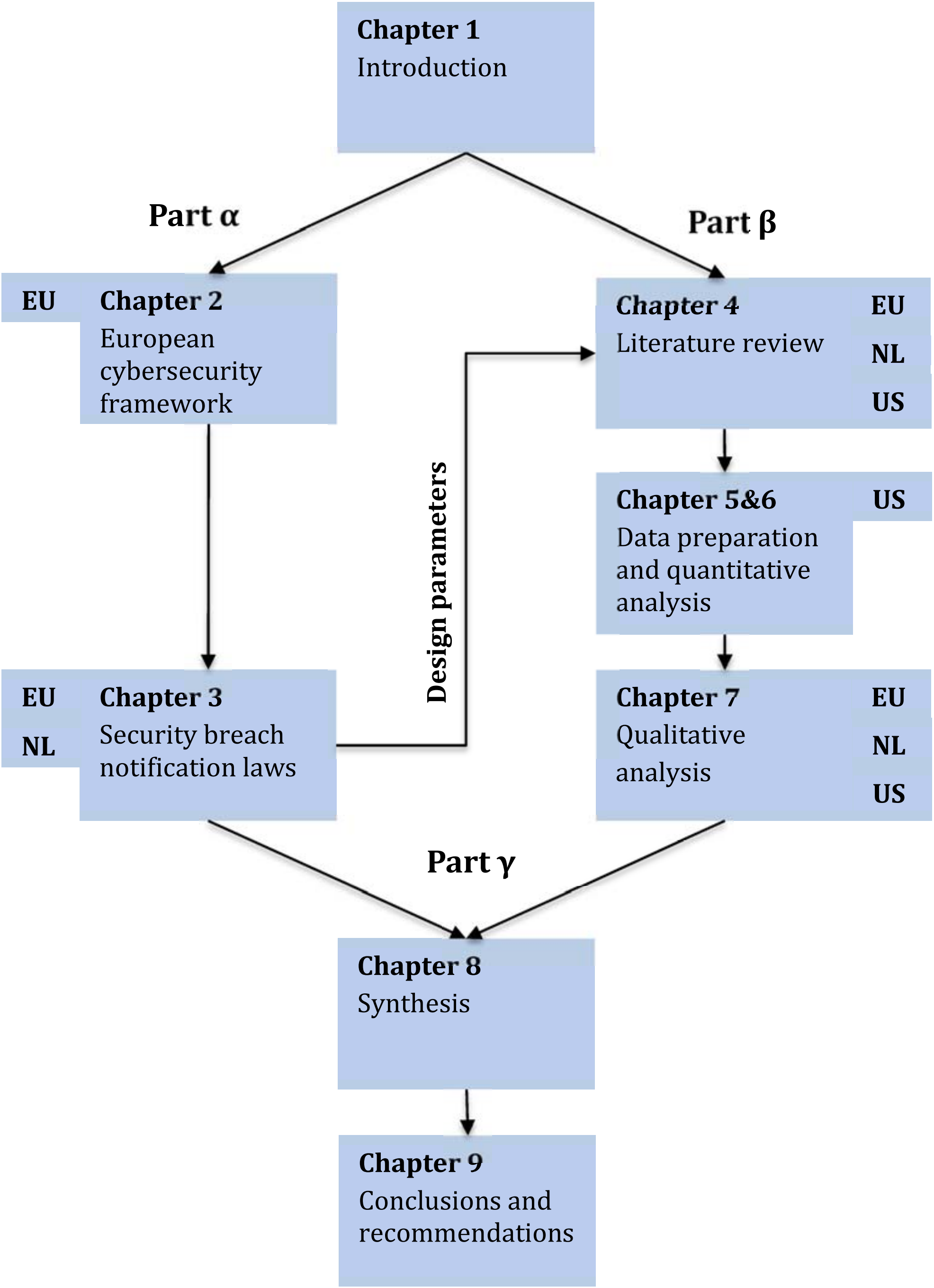


Figure 2: the approach of this thesis

Part α: a European law perspective on cybersecurity and security breach notification laws

- A European law perspective on cybersecurity necessitates the introduction of the European Cybersecurity Framework.
- The European Cybersecurity Framework consists of a policy framework and a legal framework.
- Within the policy framework, the main goals of European cybersecurity policy are displayed.
- Within the legal framework, first, the main legal bases of European law are discussed. Second, some examples are given of important secondary law in the field of cybersecurity.
- Furthermore, the origins of SBNLs in America and Europe are introduced.
- Hereafter, the concept proportionality is developed further in relation to Article 31 PDPR and Article 14 PCD.
- The assessment of the European SBNLs results in the construction of functional characteristics of the law, which are used in part β for analyzing the first order effect of the law.
- Knowledge about effects of the SBNL is substantive input for the legal proportionality test.

2 The European Cybersecurity Framework

A European law perspective on cybersecurity necessitates a description of relevant European policy goals and laws: the European Cybersecurity Framework. In section 2.1, the European policy framework is introduced. The legal framework is introduced in section 2.3. The legal foundations of cybersecurity in the Treaties and the Charter are addressed first. The European legislator has become increasingly active to pursue the goals of the European cybersecurity policy and the objectives in the Treaties and the Charter by the adaptation of a set of rules relating to both cybercrime and cybersecurity. In section 2.4, the PDRP and the PCD, which are the main topics of discussion, are addressed. Furthermore, an example of a proposal for enhanced cybercrime legislation is given: the proposed Directive on attacks against information systems (hereafter: PDIS).

2.1 European policy framework

In this section, cybercrime will be distinguished from cybersecurity. Hereafter, an overview is given of the policy goals and actions laid down in European Union soft law.

2.1.1 Cybercrime versus cybersecurity

The concepts cybercrime and cybersecurity are both addressed in European policy documents, but are distinguished by policy makers and academic researchers.[89] Cybercrime concerns the prosecutions of criminals on the Internet while cybersecurity policy relates to the resilience of computer systems regarding cyber-attacks.

Cybercrime is defined as:

> "the intentional access without right in an information system with the intent to create material or immaterial damage."[90]

And cybersecurity is defined as:

> "the protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. Information security includes those measures necessary to detect, document and counter such treats."[91]

[89] In the Netherlands, the Dutch authorities use this strict distinction. Interview with David van Duren & Bob Rijkhoek, Policy Analysts, Ministry of Safety and Justice. (The Hague, the Netherlands, 6 November 2012).

[90] European Commission 'Proposal for a Directive on attacks against information systems and repealing Council Framework Decision 2005/222/JHA' (Proposal for a Directive) COM (2010) 517 final, Article 3.

[91] Karl de Leeuw 'Introduction', in Karl de Leeuw & Jan Bergstra (eds.), *The History of Information Security: A Comprehensive Handbook* (Elsevier, 2007) 2-3.

The police and the public prosecutor perform criminal law investigation on the Internet to trace and prosecute cybercriminals. Many stakeholders, such as companies, end-users and the government, are involved in attaining a high level of cybersecurity.[92] Hence, Cybercrime is an extension of ordinary criminal law in the virtual environment, while cybersecurity is a completely new policy area.[93] Combating crime with an Internet dimension relates to the 'ordinary' criminal investigation.

2.1.2 European policy objectives

The highlights of the European policy framework are mapped in this section from 2001. The Convention on Cybercrime was signed in 2001, and the European Union introduced cybersecurity policy in 2001 as well.[94] The cybercrime and cybersecurity policy objectives can be found in European soft law.[95] In soft law, the main goals and tasks of the European Union are mentioned that should be attained by, amongst others, the adoption of legislation.[96]

This European policy framework gradually developed since 2001. There are many relevant documents that paved the way for extensive cybersecurity proposals, such as the PDPR and the PCD. A Communication of the Commission defined cybersecurity (called Network and Information Security) as:

> "the ability of a network or an information system to resist, at a given level of confidence, accidental events or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems."[97]

The Commission communication of 2006 on a secure information society updates the strategy of 2001 for new developments, such as increased deployment of mobile services and increase Internet insecurity.[98] In 2009, the Commission proposed an action

[92] Based on interviews with David van Duren & Bob Rijkhoek, Policy Analysts, Ministry of Safety and Justice. (The Hague, the Netherlands, 6 November 2012) and Axel Arnbak, PhD student, Institute for Information Law, University of Amsterdam (Amsterdam, the Netherlands, 7 November 2012). See also: Michel J.G. van Eeten and Johannes M. Bauer, 'Security Decisions, Incentives and Externalities' (2008) (OECD STI Working Paper 2008/1) <www.oecd.org/Internet/ieconomy/40722462.pdf> accessed 14 June 2013.

[93] Paul Hunton, 'The growing phenomenon of crime and the Internet: A cybercrime execution and analysis model' (2009) 25(6) *Computer Law & Security Review* 528, 529.

[94] Convention on Cybercrime 2001; European Commission 'Communication on Network and Information Security' (Communication) COM (2001) 298 final.

[95] Article 288 TFEU lists the different types of legislative acts in the European Union

[96] Soft law is European legislation that is not legally binding, see: Linda Senden and Sacha Prechal, 'Differentiation in and through Community Soft Law', in Bruno De Witte, Dominik Hanf and Ellen Vos (eds),*The Many Faces of Differentiation in EU Law* (Intersentia, 2001), 182, 197.

[97] COM (2001) 298 final (n 94) Executive Summary.

[98] European Commision, 'A strategy for a Secure Information Society – Dialogue, partnership and empowerment' (Communication) COM (2006) 251 final; 'Proposal on a European Strategy for Internet Security' (*European Commission Roadmap*, November 2012)

plan on Critical Information Infrastructure Protection (CIIP) and adopted a revised regulatory framework for electronic communications, which included new provisions such as security breaches notifications.[99] This regulatory framework provides an overview of the most important legislation concerning the telecommunications sector.

In the last few years, the European Commission prioritized cybersecurity on the European policy agenda. In 2010, trust and security became a Chapter of the Digital Agenda for Europe.[100] The Stockholm Programme underlined the importance of a cybersecurity agenda.[101] The 2012 proposal on a European Strategy for Internet Security aims to further embed a coherent European cybersecurity policy framework in national justice and governance systems.[102] A 2013 joint Communication on a cybersecurity strategy for the European Union is currently the culmination of the previous initiatives of the European Commission.[103]

The goals of the European policy framework, synthesized from the aforementioned policy documents, can be divided in four parts. First, the European Union aims to foster cooperation and share best practices between Member States. Second, the European Union aims to stimulate increased security efforts in end-products. Third, incident response capability has to be increased in order to more effectively mitigate the impact of incidents. Fourth, it aims to increase R&D investments in cybercrime. Several platforms are constituted to pursue the aforementioned goals.[104] The most important platform in the context of this thesis is cybersecurity think-tank ENISA (the European, Network and Information Security Agency). ENISA is the Union's main body of expertise that aims to develop and enhance and monitor cybersecurity policy goals, such as a security breach notification obligation.[105] The goals and the platforms of the European policy framework are displayed in the figure below.[106]

<http://ec.europa.eu/governance/impact/planned_ia/docs/2012_infso_003_european_Internet_security_strategy_en.pdf> accessed 12 June 2013.

[99] European Commission, 'Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience' (Communication) COM (2009) 149 final

[100] 'Digital Agenda for Europe' (*European Commission*, 2013) <http://ec.europa.eu/digital-agenda/> accessed 21 January 2013.

[101] European Council, 'The Stockholm Programme – An open and secure Europe serving and protecting citizens' (Notice) [2010] OJ C 115/01.

[102] *Proposal on a Strategy for Internet Security* (n 98).

[103] European Commission, 'Cybersecurity Strategy for the European Union' (Joint Communication) JOIN (2013) 1 final.

[104] The most notable platforms of the European Cybersecurity Framework are: EISAS (European Information Sharing and Alert System), EFMS (European Forum for Member States on public policies for security and resilience in the context of Critical Information Infrastructure Protection), EC3 (European Cybercrime Centre), ENISA (European Network and information Security Agency, ITU (International Telecommunications Union) and EP3R (European Public-Private Partnership for Resilience).

[105] The proposal for a Regulation concerning ENISA gives a new five year mandate and enhanced instruments for the further development of the European cybersecurity, see: European Commission 'Proposal for a Regulation concerning the European Network and Information Security' (Proposed Regulation) COM (2010) 521 final.

[106] European Commission, 'Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience' (Communication) COM (2009) 149 final; 'Digital

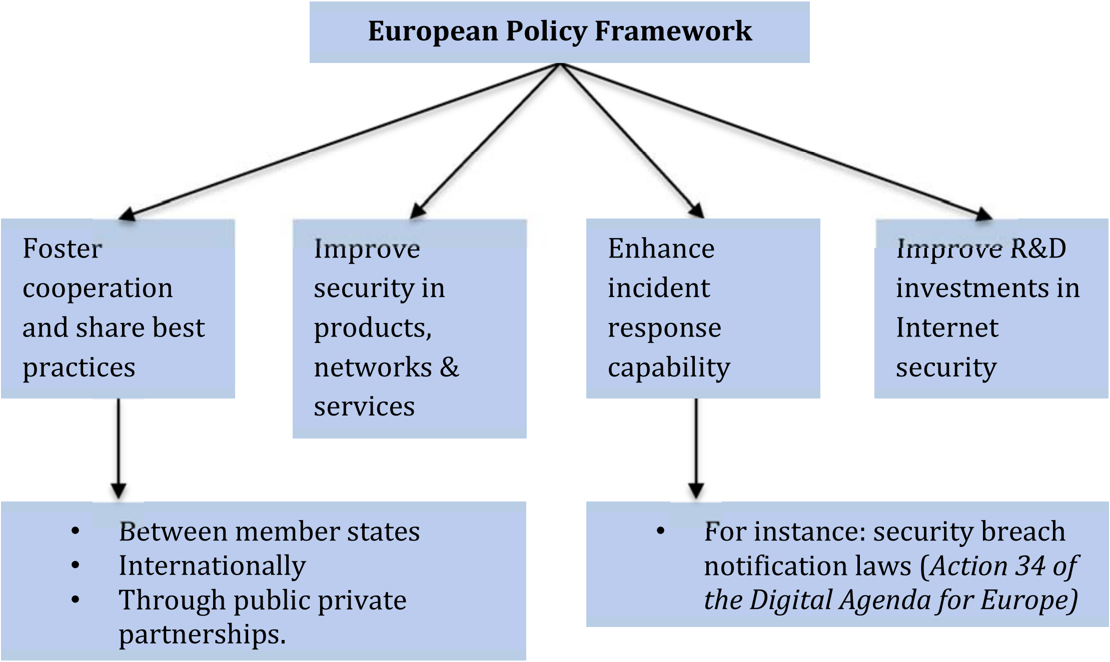

European Policy Framework
Foster cooperation and share best practices
Improve security in products, networks & services
Enhance incident response capability
Improve R&D investments in Internet security
• Between member states
• Internationally
• Through public private partnerships.
• For instance: security breach notification laws (*Action 34 of the Digital Agenda for Europe)*

Figure 3: the European Policy Framework

2.2 The European legal framework: the Treaties and the Charter

The Treaty on European Union (TEU), the Treaty on the Functioning of the European Union (TFEU) and the Charter of Fundamental Rights of the European Union (Hereafter, the Charter) are the main sources of primary law of the European Union.[107] An analysis of the sources of primary law of the European Union is necessary to assess the legal basis of the European Cybersecurity Framework. The Treaties, amongst others, constitute the structure, power and distribution of competences of the Union. Within the Charter, fundamental rights are enshrined.[108]

The European Union is a supranational institution.[109] Its 28 Member States partly gave up national sovereignty in order to achieve societal goals that were not attainable individually.[110] European law is in principle supreme over national law and legislation is

Agenda for Europe' (n 100); 'Interview Mikko Hypponen' (*Tweakers,* 20 Oktober 2012) <http://tweakers.net/video/6478/mikko-hypponen-over-cybercrime-en-digitale-oorlog.html> accessed 22 October 2012.

[107] Consolidated Version of the Treaty on European Union [2008] OJ C115/13; Consolidated Version of the Treaty on the Functioning of the European Union [2008] OJ C115/47; Charter of Fundamental Rights of the European Union [2000] OJ C364-1.

[108] The Courts case law determines to a great extent the role fundamental rights play in European Union law, see section 3.2 of this research.

[109] Graig de Búrca (n 3) 2, 3.

[110] The Member States of the European Union are (year of entry): Austria (1995), Belgium (1952), Bulgaria (2007), Cyprus (2004), Croatia (2013), Czech Republic (2004), Denmark (1973), Estonia (2004), Finland (1995), France (1952), Germany (1952), Greece (1981), Hungary (2004), Ireland (1973), Italy (1952), Latvia (2004), Lithuania (2004), Luxembourg (1952), Malta (2004),

directly applicable.[111] Supremacy means that national legislation that conflicts with European law has to be set aside.[112] Direct applicability means that European legislation, once it is adopted according to the European legislative procedure, *instantly* becomes part of national law.[113] National parliaments cannot obstruct the adoption of European law after the completion of the legislative procedure.[114] European legislation thus in principle can be an effective tool to achieve societal goals for the European Union in its entirety.

A general political debate regarding the European Union concerns the distribution of competences between the European Union and the Member States: the extent to which national autonomy should be retained.[115] The distribution of competences regarding (cyber)security is a subject of tight balancing. Member States historically demanded autonomy to determine their own legislation concerning criminal justice and national security.[116] But, the European Union is increasingly allowed by these Member States to set legislation in the field of cybersecurity, either by means of Single Market legislation, the Area of Freedom, Security and Justice or the protection of Fundamental Rights. The Single Market provisions mostly relate to the economic goals that the Internet should attain, but has also social objectives. The Area of Freedom, Security and Justice is the legal basis for cybercrime legislation. The Charter safeguards the fundamental rights relating to cybersecurity.

2.2.1 The European Single Market

The European legislator adopts rules concerning cybersecurity in the context of the European Single Market.[117] Single Market legislation aims to "integrate the national markets of the Member States into a single European market".[118] The Single Market is defined in Article 26 (2) TFEU as:

Netherlands (1952), Poland (2004), Portugal (1986), Romania (2007), Slovakia (2004), Slovenia (2004), Spain (1986), Sweden (1995) and the United Kingdom (1973).

[111] Ibid. 256-261; Case C-6/64 *Costa/ENEL* [1964] ECR 585; Case C-26/62 *Van Gend en Loos* [1963] ECR 1.

[112] Jan Jans, Roel de Lange, Sacha Prechal and Rob Widdershoven, *Europeanisation of Public Law* (Europa Law Publishing 2007), 63.

[113] The basis for direct applicability is laid down in Article 288 TFEU. The most commonly used ordinary legislative procedure is laid down in Article 289 TFEU.

[114] There is however a possibility for national parliaments to obstruct the legislative procedure as such, called the 'yellow card' of national parliaments. If one third of the national parliaments has a reasoned opinion that a draft legislative act is non compliant with the principle of subsidiarity, this draft act must be reviewed. (Article 69 TFEU; Article 6 and Article 7 of the Protocol (No 2) on the Application of the Principles of Subsidiarity and Proportionality [2007] OJ C-310/207); See also Ton van den Brink, 'The Substance of Subsidiarity: The Interpretation and Meaning of the Principle after Lisbon' in Martin Trybus and Luca Rubini (eds) *The Treaty of Lisbon and the Future of European Law and Policy* (Edward Elgar Publishing 2012).

[115] Graig and de Búrca (n 3) 291.

[116] Ibid, 926.

[117] Also called: the Internal Market.

[118] Chalmers (n 2) 674; The Single Market is sometimes also called the internal or common market.

> "an area without internal frontiers in which the free movement of goods, persons, services and capital is ensured in accordance with the provisions of the Treaties."

The European Union strives for a highly competitive social market economy (Article 3 (3) TEU). The Single Market legislation has a social and an economic objective: from an economic point of view, the absence of trade barriers and distortions of competition ought to stimulate interstate trade and consequently economic growth. An advanced Single Market should result in a level playing field for European companies in operating their businesses. This homogeneity brings economic benefits such as economics of scale because, for instance, it is much easier for companies to conduct their businesses abroad. From a social point of view, Single Market legislation harmonizes national legislation that aims to protect national interests. The European legislator can decide in which form harmonization is necessary. It can put a non-economic, social, interest in the foreground, such as public safety, provided that legislation meets the economic hurdle.[119]

The European Single Market requires cybersecurity because a secure Internet is a prerequisite for the digital economy. The European Commission explains this in the explanatory memorandum of the PCD:

> "network and information systems play an essential role in facilitating the **cross-border movement** of goods, services and people. They are often interconnected, and the Internet is global in nature. Given this intrinsic transnational dimension, a disruption in one Member State can also affect other Member States and the EU as a whole. The resilience and stability of network and information systems is therefore essential to the **smooth functioning of the Internal Market**"[120]

Internet insecurity hinders companies in operating their business. This can hinder the Freedom to Provide Services, laid down in Article 55 and 56 TFEU. In this situation, *European* legislation to align cybersecurity initiatives can be justified, because legislation by Member States individually will result in market distortions. Individual legislation, such as national SBNLs, results in different and potentially unequal treatment of companies conducting business in the Single Market. A total Single Market in the field of the digital economy has not been attained yet, because there are many obstacles for interstate digital trade, such as different data protection laws. An influential report about the Single Market led by Mario Monti concluded that: "there is a

[119] Graig & de Burcá (n 3) 607; Case C-379/98 *Germany v Parliament et Council (Tobacco Advertising I)* [2000] ECR I-8419; There can be a risk for underestimating these social interests if they conflict with the economic aims of the Single Market.
[120] *PCD* (n 4), Explanatory Memorandum.

strong demand for an effective level playing field, in areas such as the digital economy, where the Single Market does not yet exist”.[121]

The European legislator has the aim to attain the Single Market for the digital economy. There is a layered legal base for the adoption of legislation to fulfill this aim. Article 26 TFEU states the goals of the Single market, while the main legal base for adopting legislation is Article 114 TFEU. However, this legislative harmonizing power based on Article 114 TFEU is bound to limits: legislation must contribute to removing obstacles for interstate trade or distortions of competition.[122] Article 16 TFEU is important for cybersecurity legislation as well, as it concerns the protection of personal data for natural persons.[123] Article 16 TFEU can be regarded as a *lex specialis* of 114 TFEU. The regulation of data protection by the Member States *individually* can result in market distortions and suboptimal protection of individuals. The protection of personal data is also regarded as a fundamental right, enshrined in Article 8 of the Charter. [124] The two provisions have an equal value. This is stipulated by the fact that Article 16 TFEU and Article 8 of the Charter have the same formulation.[125] The importance of the establishment of cybersecurity in the context of the Single Market is also emphasized with regard to specific infrastructures, such as energy security (Article 194(1)(b) TFEU).

2.2.2 The Area of Freedom, Security and Justice

Cybercrime is regulated in the context of the Area of Freedom, Security and Justice (hereafter: AFSJ), enshrined in Title V of the TFEU.[126] The general objectives of the Union, laid down in Article 3(2) TEU, state the importance of the AFSJ.

Cybercrime is mentioned in Chapter 3 of Title V of the TFEU. This section *inter alia* regulates judicial cooperation in criminal matters. Combatting cybercrime is also explicitly mentioned as an aspect of the Area of Freedom Security and Justice in Article 67(3) TFEU: “The Union shall endeavor to ensure a high level of security through measure to prevent … crime”. Article 83(1) TFEU is a legal basis for the European legislator to establish minimum rules for *inter alia*, the fight against ‘computer crime’:

[121] Mario Monti ‘A New Strategy for the Single Market, at the service of Europe’s Economy and Society (*European Commission*, 9 May 2010), 27 <http://ec.europa.eu/bepa/pdf/monti_report_final_10_05_2010_en.pdf> accessed 13 June 2013.

[122] Chalmers (n 2) 697; *Tobacco Advertising I* (n 119) para 86.

[123] Carl-Otto Lenz and Klaus-Dieter Borchardt *EU-Verträge Kommentar nach dem Vertrag von Lissabon* (Bundesanzeiger Verlag 2010) 366.

[124] Those rights are not absolute, see: *Volker Schecke* (n 1).

[125] Lenz & Borchardt (n 123) 365.

[126] Before the Treaty of Lisbon, the European Union contained a separate pillar for Police and Judicial Co-operation in Criminal Matters. The main legal instrument of this pillar, the Framework Decision, did not have a vertical direct effect such as the Directive. The Court however stated in the *Pupino* case that Framework Decision had a form of indirect effect (consistent interpretation), which marked a tendency to increase European power in the field of security and justice. See: Case C-105/03 *Criminal proceedings against Maria Pupino* [2005] ECR I-5285, para 31; André Klip, *European Criminal Law, an integrative approach* (second edition, Intersentia 2012), 18.

> "The European Parliament and the Council may, by means of Directives adopted in accordance with the ordinary legislative procedure, establish **minimum rules** concerning the definition of criminal offences and sanctions in the areas of particularly **serious crime** with a **cross-border dimension** resulting from the nature or impact of such offences or from a special need to combat them on a common basis"

The regulation of crime and security in the context of the European Union focuses on adopting minimum rules concerning the definition and sanctioning of cybercrime. The PDIS will be discussed as a relevant example of European cybercrime law.

2.2.3 The Charter of Fundamental Rights

A secure Internet is desirable in order to guarantee non-economic values, such as the freedom of speech and the right of privacy through the protection of personal data.[127] In European law, these fundamental rights are enshrined in the Charter of Fundamental Rights of the European Union. The Charter was introduced in December 2000 as a document to show the achievements of the EU on the terrain of fundamental rights. However, its legal status remained 'undetermined' at the time.[128] With the entry into force of the Treaty of Lisbon, Article 6 TEU granted the Charter the same legal value as the Treaties. This equal legal value stressed the fact that fundamental rights form an integral part of the assessment of legislation. The European legislature must, when proposing cybersecurity laws, such as the SBNL, take into account the fundamental rights as embodied in the Charter. The PDPR is even designed to safeguard the right of protection of personal data in the Charter. The second element of proportionality principle assesses the proper balance between the aims pursued in the legislation and fundamental rights.[129]

The Charter was originally designed to reflect the existing traditional fundamental rights of the EU.[130] However, the drafters of the Charter also added other fundamental rights, which are outside the scope these traditional fundamental rights. Article 16 of the Charter for instance contains a fundamental right of the freedom to conduct business, which is not mentioned in the ECHR.

This thesis discusses the PDPR and the PCD. As said, European Union institutions must take into account fundamental rights, also when proposing legislation. This was decided far before the adoption of the Charter. In the *Stauder* case, fundamental rights are recognized as general principles of European law.[131] The Court stipulated in

[127] Daniel Drewer & Jan Ellermann 'Europol's data protection framework as an asset in the fight against cybercrime' (*Europol*, 19 November 2012), 393 < https://www.europol.europa.eu/sites/default/files/publications/drewer_ellermann_article_0.pdf> accessed 11 June 2013.

[128] Graig & de Burcá (n 3) 394.

[129] Ibid, section 3.2.

[130] Mainly the rights in the European Convention on Human Rights (ECHR).

[131] Sybe A. de Vries, 'The Protection of Fundamental Rights within Europe's Internal Market after Lisbon – An Endeavour for More Harmony' in Sybe A. de Vries, Ulf Bernitz and Stephen

Internationale Handelsgesellschaft that respect for fundamental rights forms an integral part of the general principles of law protected by the Court of Justice. The *Volker Schecke* case first gave a clear notion on the requirements for designing European legislation in relation with the obligations flowing from the Charter.[132] It states the validity of European Union Regulations must be assessed in the light of the Charter.[133] The case also stressed that unlike absolute rights such as the prohibition to torture and the right of life, most fundamental rights are not absolute, for example, fundamental rights related to Internet security, which are at issue in this thesis. These rights must be considered in relation to its function in society and thus also in relation to other aims that are achieved by means of legislation.[134]

Member States also have to take into account the fundamental rights enshrined in the Charter, just as European institutions.[135] This obligation only applies to situations when the Member States implement EU law, which is interpreted broadly (Article 51(1) of the Charter). For instance, discretionary powers conferred on Member States by a European Regulation fall within the scope of Article 51 of the Charter.[136] Member States can invoke the Charter for several reasons, for instance to justify a restriction on free movement rules by a fundamental right or by another public interest that must be interpreted in the light of fundamental rights.[137]

The PDPR and the PCD mention several fundamental rights associated with the provisions it contains.[138] The PDPR mentions the respect for private and family life protected by Article 7 of the Charter, the freedom of expression (Article 11 of the Charter); freedom to conduct business (Article 16); the right to property and in particular the protection of intellectual property (Article 17(2)); the prohibition of any discrimination amongst others on grounds such as race, ethnic origin, genetic features, religion or belief, political opinion or any other opinion, disability or sexual orientation (Article 21); the rights of the child (Article 24); the right to a high level of human health care (Article 35); the right of access to documents (Article 42); the right to an effective remedy and a fair trial (Article 47).[139] The PCD states in the explanatory memorandum that concerted practices in the context of European cybersecurity "can have a strong

Weatherill *The Protection of Fundamental Right in the EU after Lisbon* (Hart Publishing, 2013) 194; Case 29/69 *Erich Stauder v City of Ulm – Sozialamt* [1969] ECR 419.

[132] *Volker Schecke* (n 1).

[133] Ibid, para. 46.

[134] Ibid, para. 48 and for instance: case C-112/00 *Schmidberger* [2003] ECR I-5659, para. 80.

[135] Graig & de Burcá (n 3) 394. ; [2000] OJ 394; De Vries (n 131) 195; also see Article 52 of the Charter, discussed in section 3.2.

[136] See for instance: joined Cases -411/10 and C-493/10 *N.S. v Secretary of State for the Home Department* [2011] ECR I-0000, paras 64-69.

[137] See for the former situation: *Schmidberger* (n 134) and for the latter situation: Case C-260/89 *Ellinki Radiophonia Tileorassi AE* (*ERT*) *v Dimotiki Etairia Pliroforissis and Sotirios Kouvelas* [1991] ECR I-2925. There are many other cases in this intensively discussed topic. This thesis aims to examine proposals of the European legislature and therefore this situation will not be elaborated upon further.

[138] *PDPR* (n 4), Explanatory Memorandum, section 3.3.

[139] Ibid, Explanatory Memorandum, section 3.2.

positive impact for the effective protection of fundamental rights, and specifically the right to the protection of personal data and privacy."[140] In addition to that, the PCD needs to be implemented according to the Fundamental Rights in the Charter.[141]

2.3 Proposals for cybercrime and cybersecurity legislation

Secondary legislation effectuates the Union's competence fixed in the sources of primary law and is used to attain the Union's objectives.[142] As stated in section 2.2, European law has supremacy over national law. The concept of direct effect further explains the relation of secondary legislation with national law. Direct effect means that legislation directly 'confers' rights and obligations on individuals.[143] For instance, individuals may invoke directly effective legislation before the national court. The concept of direct effect thus is important to value the degree of embedment of European law into the national legal system.

Regulations have a general application and are directly effective by their nature.[144] For instance, an individual who did not receive a personal data breach notification can invoke Article 32 PDPR, if this proposed Regulation would be adopted. In the same way, the PDPR also immediately confers obligation towards data providers to notify security breaches. However, the most frequently used instrument to adopt legislation is the Directive. Directives are binding to the result to be achieved and are used for minimum harmonization of national legislation.[145] Directives impose obligations on Member States to change or adopt national law in conformity with the requirements in the Directive. Directives thus are addressed to the Member State and do not impose obligations on individuals.[146] Directives can have direct effect, but only if the provisions in the Directive are unconditional and sufficiently precise.[147] This direct effect is only vertical, in the sense that an individual can only rely on a Directive against the state, and but cannot rely on a Directive against individuals (this is called horizontal direct effect).[148] Moreover, inverse vertical direct effect (the invocation of a Directive by the state against an individual) is also prohibited. This means that any security breach notification obligations for companies flowing from the PCD must, in principle, be implemented by the Member States to impose obligations on those companies.

The European legislator has become increasingly active to pursue the goals of the cybersecurity policy by the adaptation of a set of rules relating to both cybercrime and

[140] *PCD* (n 4) Explanatory Memorandum, section 3.2.
[141] Ibid, section 3.1.
[142] Graig & de Búrca (n 3) 103; Case 93/71 *Leoniso v. Italian Ministry of Argiculture* [1972] ECR 293.
[143] *Van Gend en Loos* (n 111); Jans (n 112) Chapter 3.
[144] Article 288 TFEU.
[145] Ibid.
[146] The fact that the claim based on a Directive in a vertical relation has negative effects for a third party makes it not prohibited for an individual to invoke this Directive against the national authority, for this horizontal side effect see: Cases C-152/07 & C-154/07 *Arcor* [2008] ECR I-5959, par. 35; Jans (n 112) 78-84.
[147] Jans (n 112) 65; Case 41/74 *Van Duyn* [1974] ECR 1337.
[148] Case 80/86 *Kolpinghuis* [1987] ECR 3969.

cybersecurity. During the last decade, a number of Regulations and Directives in the field of E-commerce, telecommunications and cybersecurity have emerged. This section maps some relevant rules concerning the European cybersecurity policy. Several studies already made extensive overviews of European rules regarding to information and communication technology.[149] First, an example of cybercrime legislation is given. Hereafter, the PDPR and the PCD are discussed.

2.3.1 The PDIS and the FDIS

The PDIS is a typical AFSJ Directive that aims for minimum harmonization in the area of cybercrime, by proposing to align and update national cybercrime rules. Hence, the PDIS does not concern data protection.[150] It introduces an enhanced framework for the criminalization of cybercrime and the improvement of European criminal investigation cooperation.[151] The PDIS addresses the need to further eliminate obstacles to investigate and prosecute cybercriminals in cross–border cases.[152] The Commission argues that European assistance is needed to fight cybercrime, because connecting elements of an attack are typically situated in different locations and in different Member States.[153] Offenders have to be prevented from moving to Member States in which legislation against cyber-attacks is more lenient by means of harmonization of legislation.[154] For instance, the Directive aims to incorporate the criminalization of the latest cybercrime technology, such as botnets, in national legal systems.[155] Moreover, shared definitions of cybercrime terminology make it possible to exchange information and collect and compare relevant data.

The PDIS repeals the Framework Decision on attacks against information systems (hereafter: FDIS) because of the abolishment of this third pillar instrument after the

[149] For instance by a research of DLA piper commissioned by the European Commission, see: European Commission & DLA Piper 'Legal Analysis of a Single Market for the Information Society' (*DLA Piper*, 2009) <http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=7022> accessed 10 June 2013 ; European Commission, 'Regulatory framework for electronic communications in the European Union Situation in December 2009' (*European Commission*, 2009) <http://ec.europa.eu/information_society/policy/ecomm/doc/library/regframeforec_dec2009.pdf> accessed 10 June 2013.

[150] *PDIS* (n 90); It therefore thus not concerns data protection.

[151] Esther Meijer, 'Convention on cybercrime, Data protection in information systems through criminal law; a comparison between the EU and the US.' (Master Thesis, Utrecht University, 2012) 29

[152] Ibid.

[153] Framework Decision (FD) 2005/222/JHA on attacks against information systems [2005] OJ L 69/67, Explanatory Memorandum under 3), which is only partly implemented, see: European Commission 'Report from the Commission to the Council Based on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems (Communication) COM (2008) 448 final, Explanatory Memorandum under 3).

[154] *PDIS* (n 90) Articles 4, 5 and 6.

[155] *PDIS* (n 90) Recital 9.

Treaty of Lisbon.[156] Both the FDIS and the PDIS strongly build upon the Convention on Cybercrime of 2001, the landmark in international cybercrime cooperation.[157]
The PDIS respects fundamental rights, most notably those related to personal data and criminal justice. Recital 16 of the PDIS states the respect for "the protection of personal data, freedom of expression and information, the right to a fair trial, presumption of innocence and the rights of the defence, as well as the principles of legality and proportionality of criminal offences and penalties" in particular.

2.3.2 The PDPR and the PCD

In January 2012, the European Commission proposed the Data Protection Regulation, based on Article 16 TFEU. The PDPR concerns the protection of the general processing of personal data. The European legislature has chosen for the use of a Regulation because "The direct applicability of a Regulation in accordance with Article 288 TFEU will reduce legal fragmentation and provide greater legal certainty by introducing a harmonized set of core rules".[158] A Regulation thus makes it easier to quickly harmonize the regulation of data protection.

The PDPR updates the 'old' Directive on data protection.[159] This Directive was adopted in a time when the Internet did not have a major impact on economic and social life.[160] The Regulation imposed more obligations on the addressees of the PDPR, controllers of personal data. An example is the personal data breach notification obligation in Article 31 PDPR. However, they also "benefit from the fact that harmonization will be strengthened because of the strong harmonizing effect of the Regulation".[161] The Commission refers to the assumption that homogeneity of laws in the Single Market will bring economic benefits for companies.[162] Moreover, the data subject, the individual whose data is processed, gains more protection in the PDPR.[163] The PDPR sets rights for processing of personal data such as transparent information and communication of transfer of personal data and the right to receive a notification of a personal data security breach.[164]

Legal scholars are positive about the fundamental rights protection in the PDPR, because of extensive fundamental rights safeguards regarding the protection of personal data and privacy.[165] Article 1(2) of the PDPR provides that Member States shall protect fundamental rights and freedoms of natural persons and in particular their right to

[156] *FDIS* (n 153).
[157] Francesco Calderoni, 'The legal framework for cybercrime: striving for an effective implementation' (2010) 54(5) *Crime, Law and Social Change* 339, 344; Meijer (n 151) 29; The Convention on Cybercrime is however only ratified by 15 of the 27 EU Member States.
[158] *PDPR* (n 4) Explanatory Memorandum.
[159] Council Directive (EC) 95/46 EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995], OJ L 281.
[160] De Hert (n 61) 130, 131.
[161] Ibid, 140.
[162] See section 2.2.1 of this research.
[163] *PDPR* (n 4) Article 4(1).
[164] Ibid, Chapter 3.
[165] De Hert (n 61) 141.

privacy with respect of the processing of personal data. In theory, legal scholars are right that the PDPR indeed aims to enhance personal data control. But, there is uncertainty whether the PDPR also can achieve these aims in practice. This question will be extensively reviewed in the upcoming chapters.

One year after the PDPR, in mid-February 2013, the Commission proposed the Cybersecurity Directive.[166] The PDPR primarily focuses on the safeguarding of the fundamental right of personal data protection. The PCD focuses on ensuring a high level of network and information security across the Union. The main reason to adopt the Directive was the "insufficient level of protection against network and information security incidents, risks and threats across the EU undermining the proper functioning of the Internal market".[167] The Directive contains obligations for Member States concerning incident response mechanisms and requirements for companies to improve security. Contrary to the uniformity of the PDPR, the PCD aims to harmonize national initiatives on cybersecurity. It is up to the Member States to fill these requirements, the Directive states that companies must take "appropriate technical and organisational measures" to establish security. In the second chapter, the Directive prescribes that the Member States should define a national cybersecurity framework with concrete measures to improve Internet security. Each Member State shall establish competent authorities as a central organ to improve security.[168] The third chapter concerns structured and fostered cooperation between these competent authorities by amongst others the organization of security exercises. The fourth chapter aims security requirements and a loss of integrity security breach notification obligation. Article 14(2) PCD regulates that Member States should implement an SBNL focusing on the loss of integrity.

The PDPR and the PCD both concern SBNLs. The PDPR directly adopts an SBNL related to data protection and the PCD harmonizes national SBNLs focusing on the loss of integrity. A detailed analysis of the main aspects of SBNLs will be provided in the next chapter, which also draws attention to the relationship between the PDPR and the PCD.

2.4 Conclusions – a European cybersecurity approach?

Policy makers and academic researchers often distinguish cybercrime from cybersecurity. The aim of cybercrime policy is detecting and prosecuting cybercriminals. Cybersecurity concerns the enhancement of digital resilience. The European Union policy framework gradually developed from the beginning of the millennium and has become very extensive. The European cybersecurity policy focuses on fostering cooperation and sharing of best practices, the improvement of security in products, networks and services, the enhancement of incident response capability, and the improvement of R&D investments in cybersecurity. There are multiple platforms responsible for the coordination of those policies. The cybersecurity think tank ENISA is

[166] *PCD* (n 4)

[167] *Impact assessment PCD* (n 8), section 4.1.

[168] *PCD* (n 4) Article 6 (1); The Dutch NCSC can be regarded such a competent authority.

the Union's main body of expertise, and, perhaps, the most important platform for developing strategies concerning cybersecurity within Europe.

The European Single Market requires an increasing protection of cybersecurity and thus is a driver for the adoption of legislation. Cybercrime is regulated in the context of the Area of Freedom, Security and Justice, but the powers of the European legislature are limited to the establishment of minimum rules and cooperation. The European Charter of Fundamental rights safeguards the non-economic values associated with the Internet, such as the freedom of speech and the protection of personal data. The latter is also regulated in the context of the Single Market.

The Commission argues that the European Union has a leadership role in enhancing cybersecurity. The Commission mentions the cross border aspect of the Internet and the necessity of the Internet for the digital Single Market. Harmonization will, according to the Commission, constitute a level playing field for companies operating on the digital Single Market. Cybersecurity and cybercrime legislation, such as the PDIS and the E-privacy Directive are adopted in the context of the European Union. This demonstrates the acceptance of the European approach in cybersecurity. A broad range of cybersecurity initiatives in European soft law shows that the European Union becomes increasingly active in the field of cybersecurity.

3 Security breach notification laws

In the previous chapter, the European policy and legal framework relating to cybersecurity has been introduced. On aspect of the European Cybersecurity Framework is the security breach notification obligation. This chapter assesses the origins, proportionality and design parameters of SBNLs. Section 3.1 introduces the origins of SBNLs in the United States. The development of the European Union SBNL will be discussed along two lines, the personal data SBNL in Article 31 PDPR and the simultaneously proposed loss of integrity SBNL in the Article 14 PCD. The Dutch initiative for an SBNL is an example of a possible implementation of Article 14. In section 3.2 the proportionality requirements of the European Court of Justice will be assessed in the light of Article 31 PDPR and Article 14 PCD. In section 3.3, the similarities and conflicting differences between the European initiatives are analyzed and grouped in design parameters. Design parameters are aspects of functional characteristics of the law. The design parameters are input for literature review, the quantitative analysis on American SBNLs and qualitative analysis with Dutch experts in part β.

3.1 Origins

3.1.1 In the United States

Already at the beginning of this century, the United States started to adopt SBNLs that concern breaches of personal data. California was the first state to adopt legislation in 2002 and other states quickly followed. The company Choicepoint, which experienced a major security breach affecting 145000 people, was the first company to disclose this according to security breach legislation.[169] In 2012, forty-six states had adopted an SBNL.[170]

An example of an American SBNL can be found in the Texas Business and commerce code, § 521.03:

> "A person who conducts business in this state and owns or licenses computerized data that includes sensitive **personal information** shall disclose any breach of system security, after discovering or receiving notification of the breach, to any individual whose sensitive personal information was, or is reasonably believed to have been, **acquired by an unauthorized person.**"

In the context of this thesis, these Regulations are not important because of their legal force, but rather because their (first order) effects can be studied empirically.

[169] 'Overview Security Breaches' (*NCSL*, 2013) <http://www.ncsl.org/issues-research/telecom/overview-security-breaches.aspx> accessed 2 February 2013.

[170] Ibid.

Researchers suggest that, after the adoption of SBNLs, an increase in notified security breach incidents can be observed caused by the notification obligations.[171] Part β by will perform an analysis on the first order effect of SBNLs.

There are differences between American SBNLs. Sanctions is sometimes called 'vigorous'.[172] For instance, in Virginia the penalty for not complying with the Regulation can be 150000 dollar. On the other hand, some laws seem to be more lenient. A penalty in Washington can only be imposed in an indirect way through a civil liability action for the damage caused by failure to comply with the statute.[173] Most laws focus on informing consumers, but some also require notifying an official supervising institution.[174] Addressees are companies and governments that lost data of their customers. In some cases, encrypted data is included in the scope of the law. This variety in the design of an SBNL has resulted in initiatives to pass a federal security breach notification law.[175] The United States aims to integrate separate SBNLs, because there are coordination problems and legal uncertainty concerning the separate U.S. laws on state level. The applicability of an SBNL is based on the residency of the consumer whose personal data is breached. There are many companies with a nationwide customer base. Often, a security breach has to be notified according to multiple jurisdictions to multiple supervising authorities which causes legal uncertainty and administrative burdens.

The American laws focus on the protection of personal data and impose sanctions on non-compliance. Hence, the American laws have more similarities with the PDPR, which also includes a personal data breach criterion and can impose sanctions. The PCD and the Dutch legislative initiative focus on loss of integrity and do not impose sanctions.

3.1.2 EU: Article 31 PDPR

A general security breach notification requirement can be found in Article 31 PDPR. The aim of the PDPR is "to ensure that individuals are in control of their personal data and trust the digital environment"[176] in order to "to increase the effectiveness of the fundamental right to data protection".[177]

[171] Jan Munterman and Heiko Roßnagel, 'On the Effectiveness of Privacy Breach Disclosure Legislation in Europe: Empirical Evidence from the US Stock Market' (2009) 5838 *Lecture Notes in Computer Science* 1,2.

[172] Marne Gordan, 'When should companies go public following a security breach?' (2006) 9 *Computer Fraud and Security* 17.

[173] Washington S.B. 6043 Wa. Rev. Code, tit. 19, §255.010. (see section 5.2.2 and 5.2.4 of this research for a quantitative classification)

[174] Jennifer R. 'An Analysis of Data Breach Notifications as Negative News' (2012) 75(2) *Business Communication Quarterly* 192, 193; See for example the Idaho Statutes §§ 28-51-104 to 28-51-107. The supervising authority is in this case the Attorney General. See section 5.2.6 of this research.

[175] DLA Piper (n 149) 45.

[176] *Impact Assessment PDPR* (n 6), section 5.3.1.

[177] Ibid.

What was the reason for the European Union to adopt a security breach notification obligation?

Directive 95/46/EC and Directive 2002/58/EC impose the obligation for data controllers to ensure the security of processing of personal data. However, enforcement of these obligations is complicated, as this would require an internal assessment of the security systems of every data controller. The Commission believes that "inadequate security measures are only discovered in cases where breaches of security occur and come to the knowledge of the authorities of the public."[178] The Commission assumes that a personal data breach notification obligation results in this adequate information. Moreover, the SBNL should result in faster risk mitigation for consumers. Recital 67 of the PDPR states that: "A personal data breach may, if not addressed in an adequate and timely manner, result in substantial economic loss and social harm, including identity fraud, to the individual concerned."

The personal data SBNL has been required in the telecommunication sector since 2009. Directive 2009/136/EC, known as the E-Privacy Directive, introduced a personal data SBNL for the telecommunication providers: [179]

> "In the case of a **personal data breach**, the provider of publicly available electronic communications services shall, without undue delay, notify the personal data breach to the **competent national authority**. When the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall also notify the subscriber or individual of the breach without undue delay."

There was a need for a general legislation, because of the risk that "data breaches also exist in other sectors". [180] The Cybersecurity think-tank ENISA also advised to extend the E-Privacy Directive to have general application. ENISA pointed out the advantage of extensive data collection about security breach events because data "collected by parties such as security vendors or law enforcement agencies that have a vested interest in under- or over-reporting."[181]

This resulted in Article 31 PDPR:

> "In the case of a **personal data breach**, the controller shall without undue delay and, where feasible, not later than 24 hours after having become aware of it, notify the personal data breach to the **supervisory authority**. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 24 hours."

[178] Ibid, section 14.1.4.

[179] Article 4(2) of Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services. OJL 337/11.

[180] *Impact Assessment PDPR* (n 6), section 3.4.1.

[181] Anderson (n 48).

Article 32 requires data controllers to notify affected individuals as well:

> "When the **personal data breach** is likely to adversely affect the protection of the personal data or privacy of the data subject, the controller shall, after the notification referred to in Article 31, communicate the personal data breach **to the data subject** without undue delay."

As said, the Regulation builds on the Data Protection Directive of 1995 (Directive 95/46/EC), which did not contain a security breach notification requirement. The wording of security breach notification requirement in the PDPR is based on Article 4(2) of the E-Privacy Directive of 2009 regarding telecommunication providers.[182]

3.1.3 EU: Article 14 PCD

A SBNL focusing on loss of integrity can be found in Article 14 PCD. The Directive initiates and harmonizes initiatives for the Member States, such as the Dutch initiative on a loss of integrity SBNL.[183] The aim of the SBNL is "to create a culture of risk management and improve the sharing of information between the private and public sectors".[184] The Commission also mentions a first order aim of the SBNL: to ensure that NIS (Network & Information Security) breaches with a significant impact are reported to the national competent authorities.[185] The PCD is proposed from a (cyber)security perspective. The historical hesitance of Member States towards European Union actions concerning national (cyber)security explains the use of the less severe instrument of the Directive in the PCD.[186]

The origins of the general loss of integrity SBNL can be found in Directive 2009/140/EC. This Directive amends the common regulatory framework for electronic communication networks.[187] The Directive applies, for instance, to mobile telephone operators and thus not to every company maintaining data of citizens.[188] Article 13a contains an SBNL for telecommunication providers:

> Member States shall ensure that undertakings providing public communications networks or publicly available electronic

[182] See also: de Hert (n 61).
[183] *Impact assessment PCD* (n 8), section 4.1.1.
[184] Ibid, section 5.4.3.
[185] Ibid, annex 13.
[186] The PDPR has been approached from a personal data protection perspective, a European policy area where (total) harmonization has more political endorsement.
[187] Council Directive (EC) 2009/140 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services [2009] OJ L337/37.
[188] The Directive had to be transposed to national legislation by the EU Member States in May 2011 and is transposed in the Netherlands. The Dutch Breach notification obligation is laid down in Article 11.3a Telecommunicatiewet (Telecommunication law).

> communications services notify the competent national regulatory authority of a **breach of security or loss of integrity** that has had a **significant impact** on the operation of networks or services.

Article 14 (1) PCD states that Member States shall implement a general loss of integrity SBNL.

> Member States shall ensure that **public administrations and market operators** notify to the **competent authority** incidents having a **significant impact on the security of the core services** they provide.

It is notable that the loss of integrity SBNL only includes significant security breaches. It is however unspecified what is meant by significant. Article 15(5) provides an instruction for close cooperation of these competent authorities with the authorities responsible for the execution personal data protection. This especially applies when a loss of integrity also includes a personal data breach as is explained in the explanatory memorandum.[189] The drafters of the Directive thus saw overlap between the two types of security breaches and therefore urge the Member States to "implement the obligation to notify security incidents in a way that minimizes the administrative burden in case the security incident is also a personal data breach".

A Dutch Lowerhouse letter of 2012 contained the desire to design a general Dutch SBNL as a response to a major security breach at Dutch governmental institutions in 2011, known as the Diginotar affair.[190] This initiative fits the assignment that the PCD gives to adopt national loss of integrity SBNLs. One of the starting points of the legislation is that it should be in line with the European legislation (i.e. the PCD). The SBNL should be developed in cooperation with public and private partners and it is the responsibility of those private partners to cooperate with the government. [191]

The central organ to process the loss of integrity SBNL is the Dutch National Cyber Security Centre (NCSC) that has been operating since 1 January 2012. The core tasks of the NCSC are to build and share knowledge, enhance incident response capability and strengthen crisis management.[192]

[189] *PCD* (n 4) Explanatory Memorandum, section 1.3.

[190] 'Het Diginotarincident , Waarom digitale veiligheid de bestuurstafel te weinig bereikt' (Onderzoeksraad voor de veiligheid, 2012). <http://www.onderzoeksraad.nl/index.php/onderzoeken/onderzoek-diginotar/> Accessed 6 January 2012; 'Meldplicht Security Breaches' *Kamerstukken II* 2012/7, 26643, nr.247, 1 (letter to the Dutch Lowerhouse).

[191] Ivo W. Opstelten 'Brief Meldplicht en interventiemogelijkheden (Ministry of Safety and Justice, 6 July 2012), 2-3 <http://www.nctv.nl/Images/brief-cyber-meldplicht-en-interventie_tcm126-443885.pdf> accessed 11 June 2013.

[192] <www.ncsc.nl>.

3.1.4 Summary

The PDPR shall have direct effect and direct applicability in the Netherlands. The PCD initiates and harmonizes national initiatives such as the Dutch. The proposed legislation originates from the telecommunication Directives in 2009.

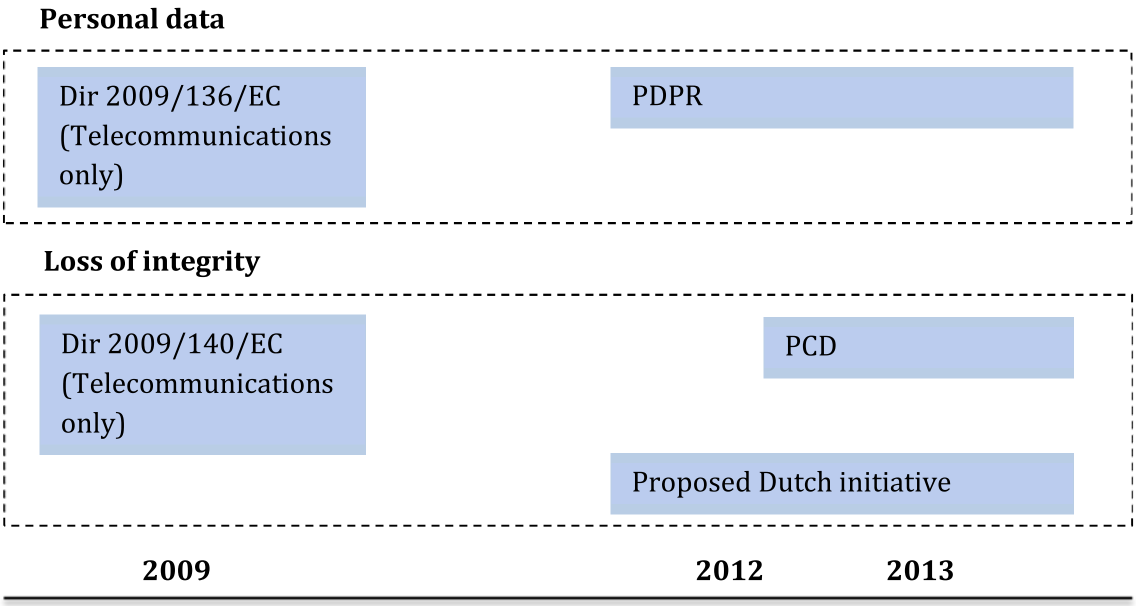

Personal data
Dir 2009/136/EC (Telecommunications only)
PDPR
Loss of integrity
Dir 2009/140/EC (Telecommunications only)
PCD
Proposed Dutch initiative
2009
2012
2013

Figure 4: European and Dutch SBNLs

3.1.5 Subsidiarity – Article 31 PDPR & Article 14 PCD

The Commission argues that there is a need for the removal of obstacles and differences between cybersecurity legislation of Member States individually, because of the cross border aspect of the Internet and the Single Market. The European legislature used the instrument of the Regulation in the DPR "in order to avoid diverging Member State rules, the Union has to provide for a harmonized system of breach notifications across the EU." The PCD also states the necessity of *European* actions: "The stated objectives can be better achieved at EU level, rather than by the Member States alone, in view of the cross-border aspects of NIS incidents and risks"[193]

The debate about SBNLs in America supports the argument of the Commission the removal of distortions in the Single Market is necessary in the European Union. The United States plans to unify state level SBNLs because the obligation to comply with multiple SBNLs simultaneously caused significant administrative burdens for companies.

3.2 Proportionality – Article 31 PDPR & Article 14 PCD

The aims of an SBNL are in the interest of both consumers and business, but paradoxally also potentially infringes the freedom to conduct business. On the one hand, there is an

[193] *PCD* (n 4), recital 40.

interest of citizens who have the right of personal data protection (Article 16 TFEU & Article 6 Charter). Moreover, both consumers and business have an interest in a secure Internet. On the other hand, there is the freedom of companies to conduct business (Article 16 Charter and in general, the Single Market).[194] A notification obligation can harm a company's legitimate interest of professional and business secrecy.[195] Apart from that, an effective SBNL can result large corporate compliance costs.[196]

How then should those conflicting interests be balanced? Article 52(1) of the Charter gives a direction on making limitations to fundamental rights, including the fundamental right of data protection (Article 8 of the Charter) and the fundamental right of the freedom to conduct business (Article 16 of the Charter):

> "any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for **by law** and respect the **essence** of those rights and freedoms. Subject to the principle of **proportionality**, limitations may be made only if they are **necessary** and genuinely **meet objectives** of general interest recognised by the Union or the need to protect the rights and freedoms of others."

The Court has assessed limitations on data protection in the *Volker Schecke* case. In *Scarlet Extended*, both data protection and the freedom to conduct businesses were analyzed. Both cases are important for the boundaries that fundamental rights sketch in European law related legislation. But, the cases have a different context. The *Volker Schecke* case concerned the validity of a European Regulation. The *Scarlet Extended* case concerned the validity of an injunction by a national court based on a European Directive.

First, the main aspects of these cases will be discussed. Proportionality is the key principle to balance interests. Therefore, the Court's approach in balancing fundamental rights will be analyzed in the light of Article 31 PDPR and Article 14 PCD according to the principle of proportionality.

3.2.1 Volker Schecke: limitations on data protection

In *Volker Schecke*, the Court assessed whether a European Regulation was in conformity with the fundamental right on data protection. The *Volker Schecke* case dealt with a European Regulation on the publication of agricultural subsidies. This Regulation had the aim to achieve transparency about the allocation of those subsidies, by publishing

[194] In assessing SBNL initiative, there is thus simple contrast between Single Market objectives and objectives of the Charter, because both interests have a legal basis in those two documents.
[195] For instance Article 41 (2) Charter.
[196] Mark Burdon, Bill Lane, Paul von Nessen 'Data Breach Notification Law in the EU and Australia, Where to now?' (2012) 28(3) *Computer Law and Security Review* 296; The societal effects of SBNLs are extensively discussed in part β.

them online.[197] The publication allegedly infringed the protection of personal data, as information of natural persons was made public in this case.[198]

The Court first assessed the legality of the limitation: the fundamental right must be limited by a Regulation that is provided by law.[199] Hereafter, the Court assessed whether the Regulation pursues an objective of general interests of the European Union. The Advocate General of *Volker Schecke*, states that these objectives needs to be very specific.[200] According to the Advocate General, the Court has to balance this specific objective of the Regulation with the infringed fundamental right(s). This is done by the principle of proportionality.

The principle of proportionality plays a key role in balancing the opposing interests that might flow from the presence of the Charter. Judicial reasoning is in most cases structured by a proportionality test.[201] To recall: the proportionality test contains two or three elements depending on case-law and legal doctrine. The first two are undisputed. First, there must be a causal connection between the measure and the aim pursued: the measure must be effective.[202] Second, there must be no less restrictive alternative available: the measure must be necessary. The last element, called proportionality *strictu sensu*, concerns "a relationship of proportionality between the obstacle introduced, on the one hand, and, on the other hand, the objective pursued thereby and its actual attainment".[203] In the *Volker Schecke* case, the Court decided to keep the test of proportionality in the form of a two-stage test of and appropriateness and necessity:

> "It is settled case-law that the principle of proportionality, which is one of the general principles of European Union law, requires that measures implemented by acts of the European Union are appropriate for attaining the objective pursued and do not go beyond what is necessary to achieve it."[204]

The Court decided that the interests were not properly balanced and that less interfering measures were not taken into account. The Regulation thus failed to pass the second element of the proportionality test.

[197] Article 44a of Council Regulation (EC) 1290/2005 on the financing of the common agricultural policy [2005] OJ L209/1 as amended by Council Regulation (EC) 1437/2007 [2007] OJ L322/1.
[198] *Volker Schecke* (n 1), para 28.
[199] Michal Bobek, 'Joined Cases C-92/09 and C-93/09, Volker und Markus Schecke GbR and Hartmut Eifert, Judgement of the Court of Justice (Grand Chamber) of 9 November 2010 N.Y.R. (Annotation)' (2011) 48(6) *Common Market Law Review* 2005.
[200] *Volker Schecke* (n 1), Opinion of AG Eleanor V.E. Sharpston, para 105. Ibid, 2009; The Advocate General provides independent and impartial opinions concerning the cases of the Court.
[201] Bobek (n 199) 2020.
[202] In legal doctrine, this causal relation is mostly called appropriate (*Volker Schecke* (n 1), para 74) or suitable. However, the more multidisciplinary term 'effective' is used in this thesis because this allows for using the same terminology in part α and part β.
[203] De Vries (n 131) 224.
[204] The "classic" full test also involves proportionality *strictu sensu*, which was not (explicitly) applied: see: *Volker Schecke* (n 1) para 74.

The Court decided in *Volker Schecke* that the institutions did not properly balance the right of privacy with the objectives of the Regulation.[205] National Courts interpret the reasoning of the Court of Justice in *Volker Schecke* as an emphasis on "the necessity to establish the most rigorous safeguards and measures for the protection of individuals when it comes to processing of their personal data"[206] The *Volker Schecke* case is important for the protection of personal data. The case favored the protection of data against the principle of transparency. National courts interpret the case as a broad Luxembourgian urge for safeguarding privacy and data protection.[207] *Volker Schecke* is in a general sense important in balancing the objectives of European Regulations and fundamental rights by means of the proportionality principle. It stimulates the European legislator to specify aims of Regulations and carry out a proportionality test upfront.

3.2.2 Scarlet Extended: limitations on the freedom to conduct business

The *Scarlet Extended* case is relevant because the Court performs a proportionality test and for the first time explicitly stresses the protection of the freedom to conduct business in Article 16 of the Charter. The Court performed a balancing test between the protection of a fundamental right to property of the intellectual property manager SABAM and the freedom to conduct business the Internet Service Provider (ISP) Scarlet.[208] SABAM, a company which represents copyright holders such as musicians and editors of musical works by authorizing their work, claimed that the copyrights of their representatives had been infringed by Internet users using Scarlet's services.[209] Internet users downloaded music without authorization and paying royalties by means of peer-to-peer networks.[210] This alleged copyright infringement was acknowledged by the Belgian court. As a consequence, Scarlet was required to install a filtering system for the preventive monitoring of the data relating to its customers in order to prevent any future infringement of intellectual property rights.[211] The Belgian court based this injunction on a discretionary power in a European Directive on the enforcement of intellectual property rights.[212]

Scarlet appealed against this decision, by stating that the effectiveness of this filtering system could not be proved, for instance because peer-to-peer networks had developed at the time and made it impossible for third parties to check their content. Moreover, it would impose unnecessary practical complications, and it would infringe upon the protection of personal data because the filtering involved the processing of IP addresses, which are personal data.[213]

[205] *Volker Schecke* (n 1) para 86.
[206] Bobek (n 166) 2022.
[207] Ibid.
[208] *Scarlet Extended* (n 12), para 46.
[209] Ibid, paras 17, 20.
[210] Ibid, para 17.
[211] Ibid, para 21.
[212] Ibid, para 30; Article 11 of Council Directive (EC) 2004/48 on the enforcement of intellectual property rights [2005] OJ L 195/16.
[213] Ibid, paras 24-26.

The Belgian Court of Appeal thus referred questions to the Court, amongst others asking for the proportionality of the filtering system. The Court acknowledged that intellectual property rights are enshrined in Article 17 (2) of the Charter, but confirmed earlier case-law that this right must be balanced against other fundamental rights. In this case, this fundamental right had to balanced with the freedom to conduct business.[214] The Court ruled that the freedom to conduct business had been infringed, because the filtering system was costly, complicated and permanent.[215] The Court concludes that therefore not a fair balance had been struck between intellectual property protection and the freedom to conduct business and therefore required filtering system should be precluded. The Courts core argument is thus the disproportional infringement of the freedom to conduct a business. However, the decision is strengthened by other arguments. First, the filtering system would also infringe the protection of personal data of the customers of Scarlet, because IP addresses need to be identified.[216] Second, the freedom to perceive impartial information is also infringed, because the filtering system might block lawful communications.[217] It is notable that the Advocate General Cruz-Villalon has a strong dissenting opinion. The Advocate General did not mention the freedom to conduct business at all and instead focused extensively on data protection and the confidentiality of communications.[218] The latter could also be infringed, next to the freedom to conduct business. In short, therefore the Advocate General also concluded that the injunction needed to be precluded.[219] This indicates the novelty of the introduction of infringement of the freedom of business by the Court as the main reason to exclude the filtering system.

Volker Schecke concerned a European Regulation and *Scarlet Extended* an obligation of the national court based on a discretionary power in a Directive as a result of a dispute between two private parties. Hence, the cases have a different context. The *Volker Schecke* and *Scarlet Extended* are both important for the boundaries that fundamental rights give when adopting legislation in a European law context. The cases stress the importance of the protection of personal data. The Court showed in *Scarlet Extended* that the freedom to conduct business is an important fundamental right as well. These fundamental rights are not absolute. However, the infringements must be proportional; effective and necessary. On case-by-case basis, it should be tested whether the European institutions indeed perform this balancing test properly. With regard to this balancing test, Advocate General Sharpston and legal scholar Bobek mentioned the specificity of the aims that the law pursues as a prerequisite for analyzing proportionality. The specificity of the aims is assessed in the upcoming section and compared with the empirically measured effect in section 8.3 of this research.

Although the cases have different starting points, they are both relevant for the proportionality test regarding Article 31 PDPR and Article 14 PCD. SBNLs have to

[214] Ibid, paras 44-46; C-275/06 *Promusicae* [2006] ECR I-271, paras 62-68.
[215] *Scarlet Extended* (n 12), para 48.
[216] Ibid, para 51.
[217] Ibid, para 52.
[218] Ibid, Opinion of Advocate General P Cruz Villalon, paras 71-73.
[219] Ibid, Opinion of Advocate General P Cruz Villalon, para 115.

respect fundamental rights, in particular data protection and the freedom to conduct business, because they aim to enhance Internet security, but impose obligations on companies.[220] The first element of the proportionality test, effectiveness, will be discussed first. Second, the necessity will be discussed in the context of the SBNLs.

3.2.3 Proportionality – Effectiveness

The first element of the proportionality test concerns effectiveness. This is the causality between the measure and the aims pursued. The effectiveness test gets limited attention by legal scholars. However, the insufficient substantiation of the aims of legislation and expected causality regarding SBNLs causes problems.

The PDPR and the PCD both mention the aims that the legislation should attain. The first order aim of the SBNL is to generate security breach notifications.[221] The second order aim of the PDPR is "to ensure that individuals are in control of their personal data and trust the digital environment"[222] in order to "to increase the effectiveness of the fundamental right to data protection".[223] The second order aim of the SBNL in the PCD is: "to create a culture of risk management and improve the sharing of information between the private and public sectors."[224]

These aims are not operationalized, they cannot be measured and it is ambiguous when exactly they are attained.[225] The fuzzy aims make it hard to perform a real effectiveness test. Article 31 PDPR aims to ensure personal data control and trust in the digital environment. How should be measured whether an obligation to notify a breach results in trust in the digital environment? And how can personal data control be 'ensured'? The PCD has the aim to create a culture of risk management and to foster cooperation between companies and the government. Achieving a culture of risk management is not a very specific objective.[226]

This conflicts with the opinion of Advocate General Sharpston in *Volker Schecke* about the need for specific aims.[227] Besides, the Commission does not substantiate in what way the proposed SBNLs will achieve the aims pursued. The Commission states that because of the nature and scale of the problems, the European actions will be more effective, but do not specify how they will be effective.

[220] The laws mention fundamental rights in their explanatory memorandum, see section 2.3 of this research.
[221] Literally mentioned in *Impact assessment PCD* (n 8), annex 12.
[222] *Impact assessment PDPR* (n 6), section 5.3.2.
[223] Ibid.
[224] *Impact assessment PCD* (n 8) section 5.4.3.
[225] Operationalization is the process of redefining an ambiguous concept to make it measurable in order to perform empirical observations.
[226] The unspecific objective as such can also cause a problem, see *Volker Schecke* (n 1) Opinion of AG Eleanor V.E. Sharpston, para 105.
[227] *Volker Schecke* (n 1) Opinion of AG Eleanor V.E. Sharpston, para 105.

Concluding, the Commission did not specify in what way the SBNL will achieve the aims pursued. Besides, the aims are not very specific and not clearly operationalized, which makes it hard to measure causality.

3.2.4 Proportionality – Necessity

The notification obligation for companies of an SBNL has similarities with the obligation for Internet Service Providers in Scarlet Extended to install a filtering system. Both impose administrative burdens on companies. In the case of a notification obligation, companies also have to disclose businesses secrets and incur reputation damage.[228] These effects might also limit the freedom to conduct business. As already mentioned, the limitation on the freedom to conduct business is proportional, if it does not impose unnecessary burdens on companies.

The Commission only limitedly assessed the administrative burdens for companies in its impact assessment, because only the costs of making a notification are included in the cost estimation. The Commission expects that the cost per loss of integrity breach notification will be 125 euro. The figure of this cost is based on 4 hour work by an employee. Furthermore, the Commission estimates that 1700 breaches will be notified per year. Therefore, the total costs for notifying breaches per year are estimated 212500 euro.[229] Moreover, the Commission also expects coordination costs because of overlap between loss of integrity and personal data breach notification obligations.[230] The Commission estimates in the PDPR that the cost of a notification is 20000 euro and expects 4000 data breach notifications to occur. These costs are based on stakeholder feedback and desk research, but are not specified further.[231] It is noteworthy that the estimations of the cost vary from 125 euro in the PCD to 20000 euro in the PDPR. This could be caused by the fact that the PDPR requires notifying individuals affected as well.

Finally, the Commission states that the PCD is not disproportionate because it imposes limited costs on its addressees, because "any of these entities as data controllers are already required by the current data protection rules to secure the protection of personal data."[232] However, contrary to this statement of the Commission, the breach notification is an additional requirement, which can also impose more extensive costs, such as reputation damage and the double notification of overlapping security breaches. Concluding, the Commission undervalues the administrative burden on companies, which questions the necessity of the current SBNL approach.

3.3 Main design parameters

The main functional characteristics of Article 31 PDPR and Article 14 PCD are mapped in this section. The four design parameters are: the addressees of the legislation, the sanctioning mechanism, the scope of the breach and the notification authority. These

[228] Chapter 5 will extensively discuss positive and negative effects of SBNLs.

[229] *Impact assessment PCD* (n 8) section 8.2.1.

[230] Ibid, annex 3.

[231] *Impact assessment PDPR* (n 6) annex 9.

[232] *PCD* (n 4) Explanatory Memorandum, section 3.2.

design parameters are used as input for the quantitative analysis on the first order effect of SBNLs in chapter 5 and 6.

3.3.1 Addressees

Addressees are the companies or personal who are addressed by the legislation. Addressees of the PDPR are all companies "processing personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system" (Article 2(1) PDPR). Processing is also interpreted very broadly as stated in Article 4(3) PDPR: "processing means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction".

The PCD applies to all market operators. The Dutch SBNL only applies to a limited amount of critical infrastructures. Currently electricity & gas, drinking water, water management and water weirs, telecommunications, the main ports Rotterdam and Schiphol, financial traffic and payment traffic. It is however imaginable that the scope will be extended to other sectors, for instance because of the eventual adoption of the PCD.[233]

3.3.2 Sanctioning & enforcement

The PDPR imposes a strict sanction for non-compliance. Penalties can be imposed for the failure to comply with two types of obligations. First, the sanction for not complying with documentation standards (Article 31(4) PDPR) of a notification can amount up to 500.000 euros or 1% of a company's world-wide turnover (Article 79(5)(f) PDPR). Second, the sanction for not notifying a personal data breach can amount up to 1 million euros or 2% of a company's turnover (Article 79(6)(h) PDPR).

The PCD does not require Member States to impose sanction on non-compliance. The Dutch initiative does not contain a sanctioning regime. They seem to be based on trust, although "competent authorities would be given the possibility to investigate cases of non-compliance".[234]

3.3.3 Scope

The PDPR mentions the scope of the breach in Recital 8: "personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed". Article 3 PDPR states that personal data means "any information relating to the data subject".

[233] *Kamerstukken* (n 190) 3.

[234] *Impact assessment PCD* (n 8) annex 3.

The PCD covers “incidents having a significant impact on the security of the core services”. The Commission states that the “the threshold for significance could be defined in relation to the impact that the breach may have on the operation of networks or services. A very important aspect in this regard is the perspective of the consumers or citizens that could be affected, and this is something that will vary from sector to sector”.[235] According to the Dutch initiative, a security breach that is likely to infringe information systems and potentially lead to societal disruption falls within the scope. This is comparable with the “significant impact on the security of the core services”. The terms will be clarified in the final legislation.

3.3.4 Notification authority and treatment

The PDPR constitutes a supervisory authority (Article 31(1) PDPR) for the notification of security breaches. The supervisory authority shall be established by the Member States according to Article 46 PDPR. The notification must be send within 24 hours after the breach. The supervisory authority shall also be responsible for a consistent application of the European SBNL.

Article 14 (2) PCD states that, in case of a security breach, the (national) competent authority must be notified. The NCSC or sectoral supervisors will be the supervising authority in the Netherlands.[236] The Dutch initiative aims to treat the initiative confidentially.[237] Confidential treatment would minimize the negative effects of reputational damage. Moreover, by treating a notification confidentially, companies can protect confidential competitively sensitive information included in a breach notification, for example details about the number of clients and competitively sensitive information.[238] The NCSC should be the main Dutch body of expertise for cooperation and information sharing. Therefore companies should have incentives to comply with the legislation, because they should benefit from this information sharing. The PCD does not mention a confidential treatment.

3.4 Conclusions

The United States were the first to establish an SBNL for personal data. The European Union followed by adopting Directives concerning personal data and loss of integrity breach notifications for the telecommunications sector. The personal data SBNL will get general applicability if the PDPR would be adopted. The PCD aims to stimulate Member States to adopt a general breach notification focusing on a loss of integrity. Before the proposal of this Directive, a Dutch legislative initiative on an SBNL concerning loss of integrity had already been introduced. The PCD directs Member States to cover all

[235] *Impact assessment PCD* (n 8) annex 2.

[236] *Kamerstukken* (n 190) 3.

[237] Interview with Jos Leenheer and Hein Verweij, Policy Analysts, NCSC, Ministry of Safety and Justice (The Hague, the Netherlands, 28 November 2012).

[238] An analogy here could be the notification of sexual abuse. People who are sexual abused are often reluctant to notify this because they are frightened for repercussions of the perpetrator. A high degree of trust in confidential treatment can give these people an incentive to notify. Apart from that, notification in anonymity such as notification points like the ‘Kindertelefoon’ and ‘Meld Misdaad Anoniem’ can be successful to overcome this reluctance.

sectors, while the Dutch initiative only covers vital infrastructures. It is however somewhat confusing that the PCD aims to attain minimum harmonization regarding loss of integrity SBNLs, while the PDPR fully harmonizes personal data SBNLs.

The cases *Volker Schecke* and *Scarlet Extended* show the European Court of Justice requires specific aims of the legislation and prohibits unnecessary infringements of for instance the fundamental right to conduct business. In contrast, the aims of the SBNLs proposed by the Commission are not very specific and operationalized. Moreover, the SBNLs impose burdens on companies, for instance notification costs that can amount up to 20000 euro. This questions the proportionality of the SBNL.

There are significant differences between the PDPR and the PCD. The PDPR focuses solely on personal data breaches and the PCD focuses on a significant loss of integrity. The PDPR can impose penalties of 1% or 2% of a company's turnover for non-compliance, while the PCD does intend to impose penalties. Some elements of the two proposals are not clear yet. The PCD has an imprecise definition of a breach. The notification authorities are not explicitly described (except for the NCSC in the Dutch initiative) and it is unclear how the European legislation will be enforced.

The two simultaneously proposed initiatives overlap, are regulated by different legal instruments and emit different signals and incentives. The European Commission confirms this overlap by admitting that a loss of integrity can also mean a loss of personal data. The simultaneous adoption of a Regulation and a Directive can create unnecessary costs for Member States because multiple supervisory authorities need to be constituted to notify a security breach. Nevertheless, the two proposals are regulated in a different way. This potentially imposes unnecessary administrative burdens for companies because they have to comply with multiple regimes. The proposals also emit different signals and incentives. For instance, the confidential treatment in the PCD will not function properly if simultaneously companies are forced to publicly disclose the same information in the PDPR.

The analysis of effects of SBNLs in part β by means of literature review, quantitative and qualitative analysis can contribute to the question whether and in which configuration the current approach is effective and necessary to attain the objectives pursued.

Part β: effects of security breach notification laws

- In part α, the origins and position of the European security breach notification law have been mapped.
- This part analyzes the effects of SBNLs.
- To structure the empirical study, a first and second order effect of SBNLs are distinguished.
- The first order effect is the effect of (characteristics of) SBNLs on the amount of breach notifications. Generating notifications is not one of the aims of the proposed legislation, but a means to achieve the second order effect.
- The second order effect includes the positive and negative effects of the law on society.
- A literature review is conducted to provide an overview of what is already known concerning those two effects.
- The quantitative analysis systematically assesses the first order effect of American SBNLs by a longitudinal dataset containing security breach notifications.
- The subsequent qualitative analysis reviews the perception of Dutch security experts and managers regarding the first and second order effect and outcomes of the quantitative analysis.

4 Literature review on effects

This chapter concerns a literature review on the effects of SBNLs. The following causal structure has been introduced to distinguish the focus of the three types of analysis on the effects of SBNLs. This literature review introduces an analysis of first and second order effects of SBNLs.

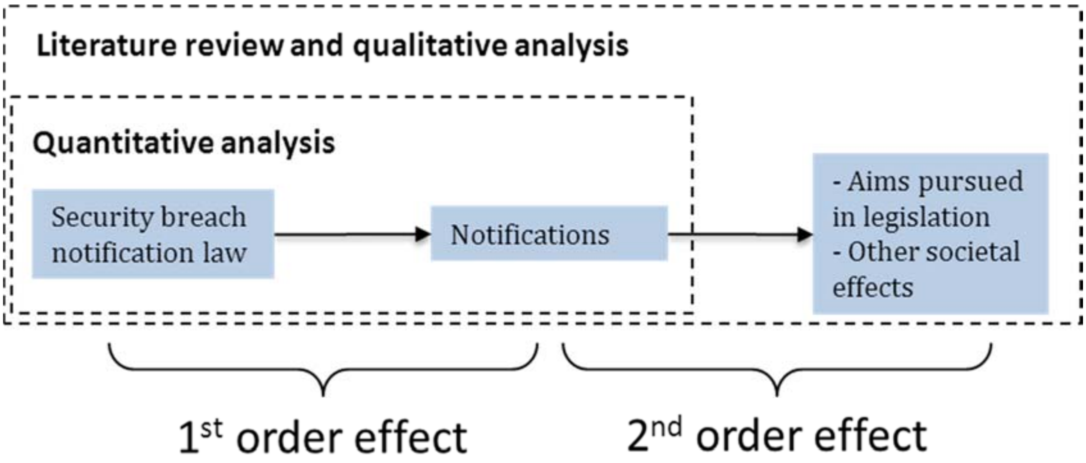

Literature review and qualitative analysis
Quantitative analysis
Security breach notification law
Notifications
- Aims pursued in legislation
- Other societal effects
1st order effect
2nd order effect

Figure 5: first and second order effects of SBNLs

The effects are mostly derived from American literature, where the topic is discussed extensively and where there is a long experience with SBNLs. The analysis is used to enhance the proportionality test of proposed SBNLs in the European Union.[239]

The first order effect of SBNLs entails the relationship between design parameters of a law and the amount of notifications from companies experiencing a security breach. This mostly concerns compliance with the law. Compliance will be interpreted as notifying a security breach within the scope of the law. The regulatory compliance theory provides a framework to discuss incentives for actors to comply with the law. Within this subject, there is a short intermezzo about cost of compliance compared to withholding a security breach. These incentives for compliance can be used to draw hypothesis in the quantitative analysis.

The second order effect includes the positive and negative societal effects of SBNLs, including the aims pursued in legislation. In literature, there are analytical suggestions and empirical measurements about the second order effects of an SBNL.[240] The second

[239] The European proposals entail the constitution of a new legal institution, which probably has different effects than the experience in the United States. Moreover, this research concerns human behavior on different levels, such as the individual level, organizational level and national level. Al these levels generate a different type of behavior, which will lead to incentives to notify of withhold a notification. The real world of making a notification is thus inherently more complex than the causal structure presented that serves as a basis for subsequent empirical analysis.

[240] Moore (n 73) 584.

order effect will be discussed in this literature review and in subsequent qualitative analysis.

4.1 First order effect

In this section, compliance will be discussed. Knowledge about compliance is important to understand what drives companies to notify a security breach.

4.1.1 The regulatory compliance theory

The regulatory compliance theory provides assumptions for the motivation of actors to comply with legal obligations.[241] This theory provides knowledge about the underlying reasons for companies to make notifications.[242] Ayres and Braithwaite were the first to distinguish profit maximization (the logic of consequences) and morality (the logic of appropriateness) as main motivations for compliance.[243] These motivations both play a role in the consideration to notify, but their relative importance can vary. A traditional rational actor has profit maximization as a main motivator and will perform a rational cost benefit analysis when the decision to notify or withhold a notification must be considered. An actor that has morality as a main motivation assesses whether the law is appropriate according to internalized moral norms.[244] In this situation a negative cost benefit analysis still can result in compliance. There is empirical evidence that a significant part of compliance cannot be explained by rationality but is explained by morality.[245] The main motivation of an actor steers a compliance decision. For instance, an actor that is non-compliant because of the immorality of the law will not be very sensitive for higher sanctions. Rationality and morality thus both play a role in compliance theory. They can also play a role in complying with SBNLs. A purely rational actor would comply with an SBNL if the costs of compliance are lower than the costs of non-compliance. A rough estimation of the cost of compliance is provided in section 4.1.3. A purely moral actor would comply with an appropriate law that contributes to Internet security.

4.1.2 Incentives for compliance

Enforced sanctions and benefits from information sharing are rational incentives that have a positive effect on compliance. High sanctions in combination with a vigorous enforcement increase the cost of non-compliance. The exchange of information and best

[241] For example used by: Tom R. Tyler, 'Compliance with Intellectual Property Laws: A Psychological Perspective' (1999) 29 *New York University Journal of International Law and Politics* 219; Julien Etienne 'Compliance Theory: A Goal Framing Approach' (2011) 33(3) *Law & Policy* 305; Durwood Zealke, *Making Law Work, Environmental Compliance & Sustainable Development* (International Law Publishers 2005) 53.

[242] Compliance thus is defined in the broad sense by making notifications when a notification law is adopted.

[243] Ian Ayres & John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (Oxford University Press, 1992).

[244] For instance: Fisherman did not fish illegally despite the fact that illegal gains were much larger than expected penalties; they found the law moral just, see: Etienne (n 241) 308.

[245] Jon Sutinen and K. Kuperan, 'A socio-economic theory of regulatory compliance' (1999) 26 (1/2/3) *International Journal of Social Economics* 174.

practices can give companies incentives for compliance because they benefit from this information.[246] Many researchers suggest that reputational damage is a strong negative driver for companies.[247] Reputation damage and subsequently loss of trust by consumers and competitive power are costs of compliance. Next to rational incentives, the regulatory compliance theory distinguishes moral incentives for compliance. Companies can be morally bound to comply with SBNLs because it contributes to Internet security. Empirically, there is little information on how the various incentives affect compliance with SBNLs. Research on the effect of the strictness of a law on identity thefts did not find a significant effect.[248]

Key incentives for compliance in literature

- Positive
  - Enforced sanctions
  - Benefits of information sharing
  - Contribution to Internet security (appropriateness)
- Negative
  - Reputation damage

4.1.3 Intermezzo: rough analysis of the cost of compliance

This section provides a rough estimation of the cost of compliance and the cost of non-compliance of the American SBNL and the PDPR. The calculation assumes that companies solely balance enforced sanctions with reputation damage in their consideration. Therefore, compliance would result in costs of reputational damage and non-compliance would result in expected costs of possible reputational damage and penalties.

There is no clear consensus on the effects of reputation damage. Goel and Hawsky estimated a 1% loss of market value, which is used in this calculation as an assumption of the reputational cost.[249] The PDPR imposes sanctions for non-compliance that can amount up to 2% of the worldwide turnover of a company. The cost of compliance of the PDPR is compared with the SBNL in Michigan. The Michigan SBNL is one of the most vigorous; it has the highest predetermined sanction of 750000 dollar. The calculation assumes that both states impose the maximum penalty. Moreover, a likelihood of apprehension of 10% can be regarded as an optimistic estimation of the enforcement powers of a supervising authority.[250] In addition to that, breaches can also be disclosed by third parties and probably also will result in a penalty. This likelihood of an

[246] Mulligan (n 54) 21; Jane K. Winn 'Are 'Better' Security Breach Notification Laws Possible?' (2009) 24(3) *Berkeley Technology Law Journal* 1133.
[247] For instance: Sanya Goel and Hany A. Hawsky, 'Estimating the market impact of security breach announcements on firm values' (2009) 46 *Information and Management* 404; see also section 4.2 of this research.
[248] The others place question marks at the limited sample size of this observation.
[249] Goel and Hawsky (n 247).
[250] (In fact this is probably much lower, because our database contains a list of breaches of 0.05% of American companies while there are estimations that 42% of the companies suffered a data loss.).

unintended disclosure is estimated to be 20%. Furthermore, it is assumed that the company concerned has a price to sales ratio of 5:1 and a turnover of 10 million dollar. The expected cost of compliance and non-compliance are displayed below.[251]

Expected cost of compliance and non-compliance per breach

- Cost of compliance (reputational damage)
  - European Union: 500000 dollar
  - Michigan: 500000 dollar
- Cost of non-compliance (possible reputational damage and possible penalty)
  - European Union: 210000 dollar
  - Michigan: 375000 dollar

In this situation, the costs of compliance are higher than the costs of non-compliance. This is mostly due to the fact that the likelihood of being caught for non-compliance is estimated as low, because it is assumed that enforcement is difficult. As Winn states: “If there is no compliance mechanism to be detected, there is no economic incentive to comply with a law, when compliance would be very costly.”[252] However, this calculation relies on a few contestable assumptions, such as the height of reputational damage, the likelihood of apprehension and the imposition of a maximum sanction. Hence, it demonstrates that high reputational damage in combination with a low likelihood of apprehension make economic incentives to comply absent, even if high sanctions are imposed for non-compliance.

4.2 Second order effect

An SBNL can have various societal effects. The problem of cybersecurity economics is characterized in the introduction. Scholars have suggested effects of SBNLs and partly provide qualitative and quantitative empirical evidence.[253] The positive effects of SBNLs can contribute to the mitigation of the problem of cybersecurity economics. As stated in the introduction, the problem has the following characteristics.[254]

- Imperfect information about effective security measures because of the complexity of big data and defense systems.
- Negative externalities on society concerning the costs of security breaches.
- Underpowered incentives to invest in security, protect consumers information and share knowledge with competitors.

An SBNL aims to generate (more) security breach notifications. According to scholars, this results in an increase of information and awareness about security breaches and in an strengthening of incentives to invest in security, protect consumer information and

[251] A calculation is provided in Appendix D.
[252] Winn (n 246).
[253] Moore (n 73) 584.
[254] See section 1.1.4 of this research.

share knowledge about security best practices. On the other hand, an SBNL can also result in high maintenance and compliance costs for governments and companies.

Romanosky expects that both firms and consumers gain increased incentives to avoid breaches as soon as they become aware of their existence.[255] He calls the deterrent effect of disclosing a security breach: "Sunlight as a disinfectant". Romanosky analyzed the impact of American SBNLs on the amount of identity theft reports from the U.S. Federal Trade Commission and found an average reduction of 6.1% in fraud rates after a state adopted an SBNL. Winn places these statements in perspective by stating that the sunlight as disinfectant principle mostly has negative effects for companies: "the shaming function of SBNLs is direct and concrete, while any incentive they [the laws] provide to improve security is indirect and uncertain." Winn expects actors to act rationally, and regards enforcement of non-compliance in the U.S. as weak and benefits as indirect and uncertain. Consequently, he projects that SBNLs generate little compliance and subsequently impact on society.

Contrary to the pessimistic view of Winn that the SBNLs will have little impact, Romanosky argues in addition to the "Sunlight as disinfectant" principle that consumers should have a "right to know" that their data is lost. Schwartz en Janger suggested that this right to know and especially the subsequently quick awareness of a security breach by consumers have positive impact on mitigating losses.[256] Mulligan derives relevant observations from interviews with chief security officers of a number of large American firms. They are positive about the effects of SBNLs and also perceive consumer awareness to be heightened.[257] More general, they perceived that "notification laws have raised the level of awareness of the importance of information security" and "have fostered cooperation between information security departments".[258] Moreover, they confirm the sunlight as disinfectant principle by perceiving an incentive for security enhancement: "fear of reputation damage, in addition to the notification requirement itself, drives organizations to take steps to at least evaluate, if not correct and enhance, security mechanisms".[259] They also underlined the benefits of information sharing: "security breaches at other organizations provide CSOs with information on new and developing forms of threats"[260] and "responsibility for the loss of personal information has resulted in an informal system of industry self-regulation, as organizations are not only strengthening security, but are requiring that other organizations that handle their data meet their standards as well".[261]

The reputation damage that companies experience after a security breach has been made public has been the subject of frequent empirical measurement. Reputation

[255] Sasha Romanosky, Rahul Telang, Allesandro Acquisiti, 'Do Data Breach Disclosure Laws Reduce Identity Theft?' (2011) 30(2) *Journal of Policy Analysis and Management* 256, 262.
[256] Paul M. Schwartz and Edward J. Janger, 'Notification of Data Security Breaches' (2007) 105 *Michigan Law Review* 913, 971.
[257] Mulligan (n 54) 24.
[258] Ibid, 4.
[259] Ibid, 14.
[260] Ibid, 21.
[261] Ibid, 22.

damage is estimated by measuring the value or performance of companies before and after a notification. Goel and Hawsky estimated the impact of security breach announcements on firm values. They used event study methodology to study breach events from the media. A few days before and after the notion of a security breach, the market value of a company was measured.[262] They found a negative impact a few days after the breach, on average about 1 % of the market value. Cavusoglu identified through a similar approach an incidental loss of stock prices of 2.1%.[263] Ko and Dorantes used a matched sample comparison analysis instead of event study methodology to investigate the impact of security breaches on firm performance.[264] The results suggested "that information security breaches have minimal long-term economic impact" There is thus not a clear consensus of the long-term effects of a breach. However a breach does likely effect market value on the short term.

A vigorous enforcement regime and many notifications to be processed can result in high social costs. Governments incur costs for maintaining and constituting the enforcement and notification processing system. Companies incur costs in complying with the law, for instance to assign employees to the process of notifying.[265] If the probability of a security breach is low, but enforcement high, companies can make unnecessary costs by overreacting by for example constantly review credit cards of customers. [266]

Key effects of SBNLs discussed in literature

- Positive
  - "Sunlight as a disinfectant": increased investments in security by company and consumers
  - "Right to know": awareness of consumers of security breaches
  - Fostered cooperation between companies
  - Faster risk mitigation after a breach
- Negative
  - Companies: (fear for) reputation damage for companies
  - Governments: societal costs of processing, enforcement
  - Companies: increased investments, fostered cooperation and compliance

[262] Goel and Hawsky (n 247).
[263] Huyesin Cavusoglu, Birenda Mishra and Srinivasan Raghunathan, 'The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers' (2004) 9(1) *International Journal of Electronic Commerce* 69.
[264] Myung Ko, and Carlos Dorantes, 'The impact of information security breaches on financial performance of the breached firms: an empirical investigation' (2006) 16(2) *Journal of Information Technology Management* 13.
[265] Winn (n 246) 1135.
[266] Romanosky (n 255) 260.

4.3 Conclusions

This chapter has outlined the discussion in literature about the first and second order effect of the SBNL. According to the literature, the design of notification laws determines the magnitude of the first order effect; the amount of notifications. Sanctions, benefits from information sharing and appropriateness give incentives for compliance. Reputational damage gives incentives for non-compliance. The cost of compliance is possibly higher than the costs of non-compliance. As a consequence, a rational actor, as specified in section 4.1.3, will not comply with a notification law. The reservation should be made that this cost calculation is based on contestable assumptions, for instance relative low enforcement and high reputational damage. The incentives for compliance that are identified in this chapter, are essential information for drawing hypotheses in the subsequent quantitative analysis in section 5.3.

A number of important societal (second order) effects of SBNLs are developed. There are positive effects, such as increased security investments and awareness. There are also negative effects, such as costs of the notification system and administrative burdens of companies. These effects are important because they form a substantive input for the proportionality assessment of the European Union legislative proposals.

5 The dataset

This chapter prepares a dataset in order to test whether characteristics of American SBNLs affect the amount of breach notifications. The United States of America have adopted general applicable SBNLs since 2003. This is different from the European Union and the Netherlands, where legislation is in the design phase.[267] The American laws focus on loss of personal data and thus have the most in common with the European Union proposal on the protection of personal data. The aim of this and the subsequent chapter is to learn from this American data in order to make recommendations for the PDPR and the PCD. The dataset, which contains empirical data about security breaches, can assist in understanding whether these classifications relate to compliance. Indeed, if an SBNL is effective in causing more breaches, this in principle can be identified by an increase of the amount of security breaches in the dataset.

In section 5.1, the dependent variable is constructed: security breaches per firm per state per year. The dataset, from which the dependent variable is constructed, is introduced first: the Privacy Rights Clearinghouse dataset, which contains security breaches from 2005 until 2012. The dataset concerns longitudinal data: data of multiple subjects (states) with multiple measurements in time (years). Second, the dependent variable is developed by restructuring the data. Attention is paid to omitted variables between states and and over time that can influence the dependent variable. This discussion results in the decision to control for the amount of firms in a state.

In section 5.2, the American SBNLs are classified based on 6 aspects that cover the design parameters sanctioning, scope and notification authority constructed in chapter 3. These classifications are the independent variables of the quantitative analysis that will be executed in the next chapter.[268]

5.1 The dependent variable: security breaches per firm per state

With some exceptions, U.S. supervisory authorities do not record the amount of official notifications flowing from the legal obligation to notify.[269] The intended quantitative analysis thus has to rely on secondary data of organizations that collect and register security breaches. The dataset of a Californian nonprofit organization, called the Privacy Rights Clearinghouse, is used for this purpose. The goals of this organization are *inter alia* to "document the nature of consumers complaints" and "answer questions about privacy in reports, testimony, and speeches and make them available to policy makers, industry representatives, consumer advocates and the media."[270] A part of this work is

[267] See section 3.1.2 of this research for the European Union SBNL for telecommunication networks.

[268] The software package IBM SPSS Statistics is used to perform the analyses.

[269] 'The Privacy Rights Clearing House DataBase' (*PrivacyRights.org*, 2013) <https://www.privacyrights.org/data-breach> accessed 1 February 2013.

[270] Ibid, under: 'About us'.

the maintenance and construction of a dataset containing security breaches. The dataset has strengths and weaknesses. A strength is that the Privacy Rights Clearinghouse database only registers U.S. security breaches and that all U.S states between 2005 and 2012 are covered.[271] The 3554 breach reports contain several characteristics of a security breach, such as a resume of the breach, the amount of records breached and the sector, the state and year in which the breach occurred.[272] A weakness is that the dataset is an aggregation of multiple security breach databases (hereafter: sources). Those sources are not mutually exclusive as they can contain the same breaches. However, duplications have been filtered out. Apart from that, some sources are added in a later stage of the data collection, which can give a false impression of an increased number of security breaches over time. Moreover, the representativeness of the data is questionable: less than 0.05% of the U.S. companies is represented, while it is likely that a multiple of that suffered a security breach between 2005 and 2012. Besides, several actors, such as companies, consumers and third parties can be the reporters of a breach, while the interest of this research solely lies at companies that notified their own breaches in order to make statements about compliance with the law.[273] The Privacy Breach Clearinghouse, however, claims that most of the breaches come from the harmed companies by stating that "if a breached entity has failed to notify its customers or a government agency of a breach, then it is unlikely that the breach will be reported anywhere".[274] For this research, the official fifty US states will be used for analysis. Thus, the District of Columbia, Puerto Rico and the Virgin Islands are omitted from the database.

Breach: an occasion of a security breach.
Record: the amount of people affected by a breach.
Source: the underlying database that collected the breach.

5.1.1 Description of the security breaches in the database

A descriptive analysis of the characteristics of a security breach in the dataset for the year 2012 shows that the size and fashion of security breaches widely varies. In 2012, 675 breaches were registered. In most of the cases, a breach contains multiple records: the amount of people affected by the breach. The size of the breach varies between a few records and millions of records. There are small breaches (less than 1000 records), medium size breaches (between 1000 and 10000 records breached) and large breaches (more than 10000 records per breach). The size of 246 breaches is unknown. Almost all states have small, medium and large breaches. California, for instance, contains 122 breaches. This varies from 15 affected people (A hospital employee that used credit card information of cancer patients) to a big LinkedIn data breach, which contained 6.4 million encrypted passwords that were posted online by a group of hackers. In

[271] Ibid.

[272] The breaches are classed by sector: businesses (retail, financial/insurance and other), educational institutions, government and military, healthcare and non-profit organizations.

[273] Firms notify a their own breaches, but customers and third parties notify suspicious information on the Internet.

[274] The Privacy Rights Clearing House DataBase (n 269).

Washington, 16 breaches were reported: the smallest breach reported consists of 16 records (a small credit card fraud). The largest breach affected 35 million people by hacked password information an online gaming platform. In Virginia, there were also small breaches, such as a breach with 30 records in November 2012 in the healthcare sector. The largest breach (176567 records) contained a security hack of the server of Virginia Commonwealth University that contained personal information of former and current employees, students, staff and affiliates. Some breaches only include records such as passwords from a particular website such as the LinkedIn data breach, while in other cases people are affected directly, for example through the use of stolen creditcard information for fraudulent activities. Therefore, the number of records breached is not a very accurate unit for the impact of the breach. Based on this analysis, a smaller breach generally has a higher impact per record than a larger breach, but larger breaches compensate this by a multiplicity of records. The European Commission confirmed this observation in the impact assessment of the PDPR:

> "The number of individuals concerned by a breach cannot be used as a severity criterion, as the possible risk for any individual is not dependent from the number of others that are concerned by the same incident. In some circumstances damage may even be more likely when less individuals are concerned, e.g. if a hacker obtains only a few credit card records, each one may have a much higher probability to be used for fraud than when several million records are stolen."[275]

Below, the distribution of all breaches is given for 2012 and the entire dataset. It shows that most breaches are not categorized and that the size of breaches is distributed fairly evenly. In the eight-year period observed, in total, 600 million records were breached. The three largest breaches contain more than 300 million records.

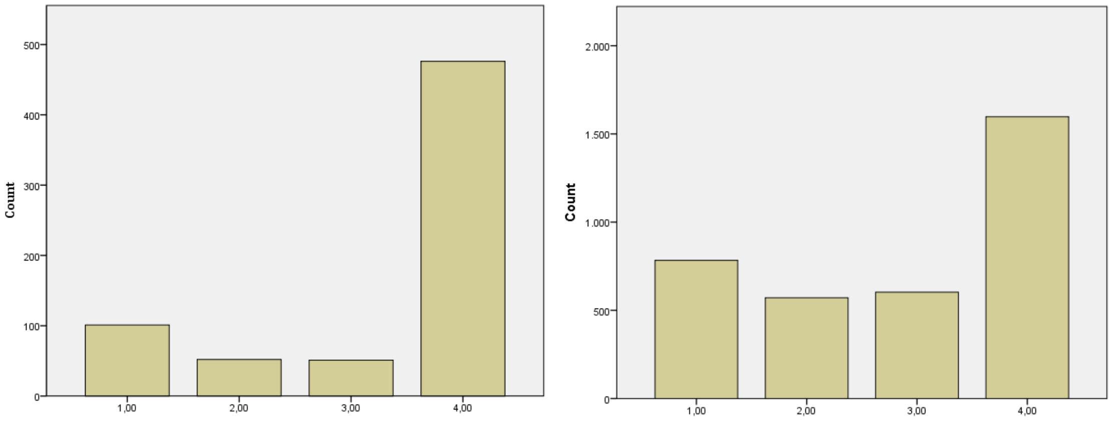


Figure 6: total records in 2012 (left) and 2005-2012 (right) (1=0-1000; 2=1001-10000; 3=10001+; 4=unknown)

[275] *Impact Assessment PDPR* (n 6), section 14.1.4, under 4).

5.1.2 Sources of the database

The database is an aggregation of several security breach notification sources. The amount of notifications per source and the representation of the sectors are shown in the figures below:

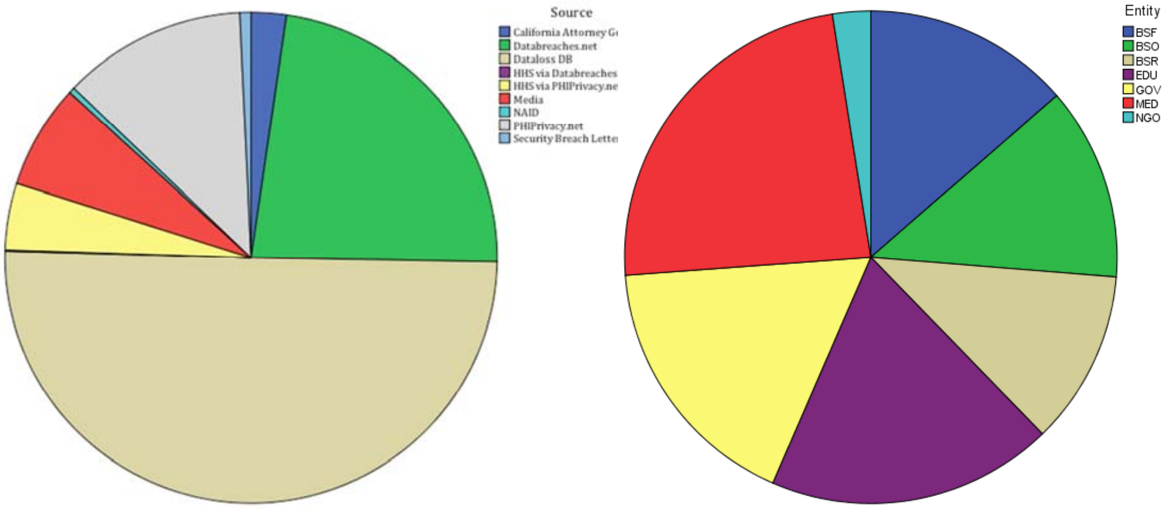


Figure 7: different sources in dataset from 2005 until 2012 and sectors.[276]

Most of the breaches come from the Dataloss DB database. As of January 2010, the sources Databreaches.net, PHI Privacy and NAID are included. As of March 2012, the list of the California Attorney General is included.[277] As said, the sources are not mutually exclusive, which entails that one occasion of a security breach can both be found in Dataloss DB, the media, and by the Attorney General of California. PHIPrivacy, ‘HHS via’ and NAID mostly include medical breaches, which is also problematic from a representativeness point of view. Herafter, two examples of sources that are not representative are displayed: the source ‘California Attorney General’ represents mostly breaches from California and PHIPrivacy.net contains mostly breaches in the medical sector.

[276] The sectors are labeled as follows: BSO - Businesses – Other; BSF - Businesses - Financial and Insurance Services; BSR - Businesses - Retail/Merchant; EDU - Educational Institutions; GOV - Government and Military; MED - Healthcare - Medical Providers; NGO - Nonprofit Organizations.

[277] The Privacy Rights Clearing House DataBase’ (n 269) under ‘FAQ’.

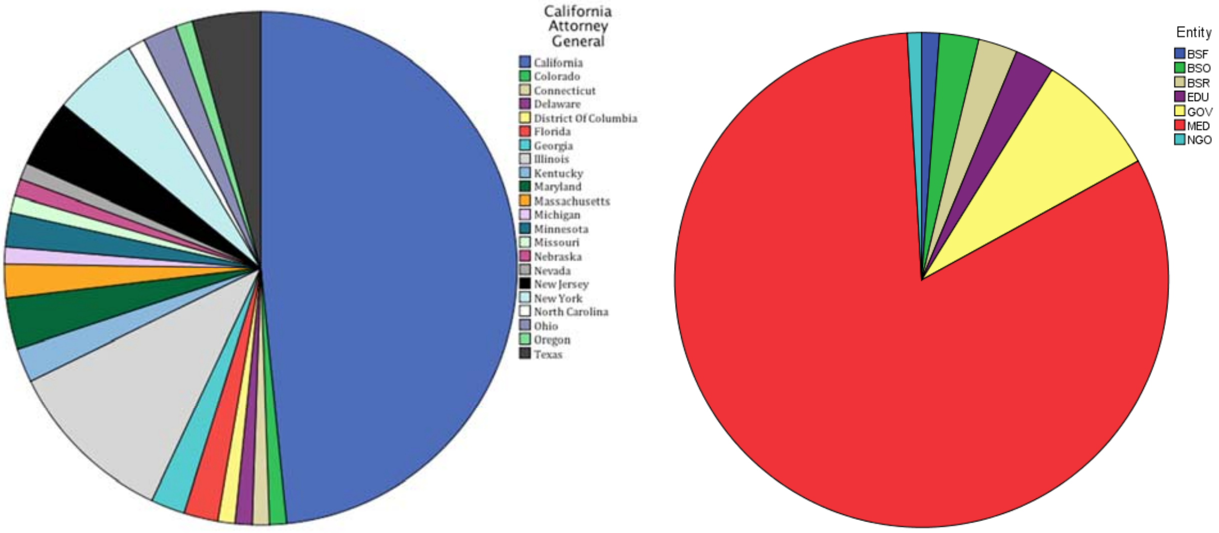


Figure 8: representativeness issues: breaches per state from the source 'California Attorney General' and sector of breaches of PHIprivacy (medical is red).

Although the database does not contain duplications, the exclusion of sources that are not representative for the population or added in a later stage could be problematic. Breaches in the sources that are not representative can originally also be represented in sources that are representative, before they were filtered out because of the duplication exclusion. Those breaches would be falsely excluded if the sources that are not representative would be excluded. The risk of falsely excluding breaches at the one hand and representative issues of some sources at the other hand emerged. Therefore, a two-track approach is adhered to systematically mitigate this risk. This consists of the construction of two separate dependent variables. The first is based on all sources and the second is based solely on the breaches that come from Dataloss DB and databreaches.net. These two sources are selected because they are the two largest sources, clearly overlap and do not have striking representativeness issues. The distribution of the sectors of the database with the selected sources looks as follows.

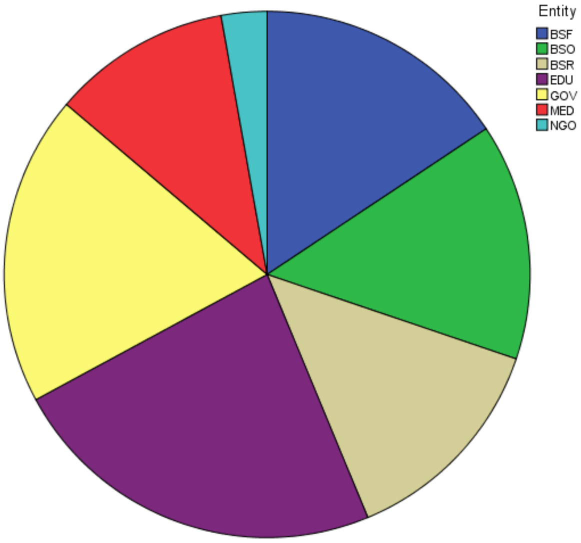


Figure 9: distribution of sectors of selected sources

5.1.3 Restructured data: breaches per year and per state.

In order to analyze breaches per year and per state, the raw database is restructured into a list of 400 cases containing the amount of breaches per state for each year between 2005 and 2012. (50 states containing 8 years of data) [278] The following graph only displays year after year effects. The total amount of breaches of 50 states is summarized per year.

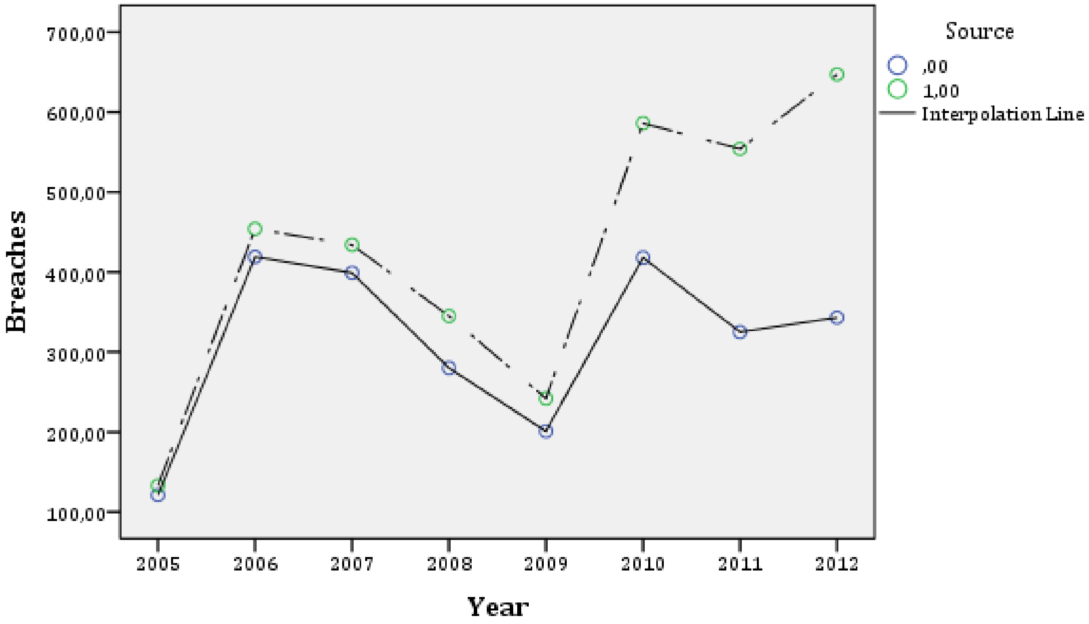


Figure 10: breaches per source (0=selected sources; 1=all sources)

An inconstant increase of the amount of notifications can be observed. It must be noted that from 2010 on, the new sources that were added to the database can explain the increase of notifications. Apart from this, a remarkable decline is visible in 2008 and 2009. This could be related to the financial crisis, although this remains speculation. The following graph represents the amount of records per source per year. It is clearly visible that the Dataloss DB and databreaches.net sources overlap. This overlap is one of the reasons that the two sources are selected together.

[278] The raw database contains of 3554 cases (all sources included) or 2506 cases (selected sources: Dataloss DB and Databreaches.net).

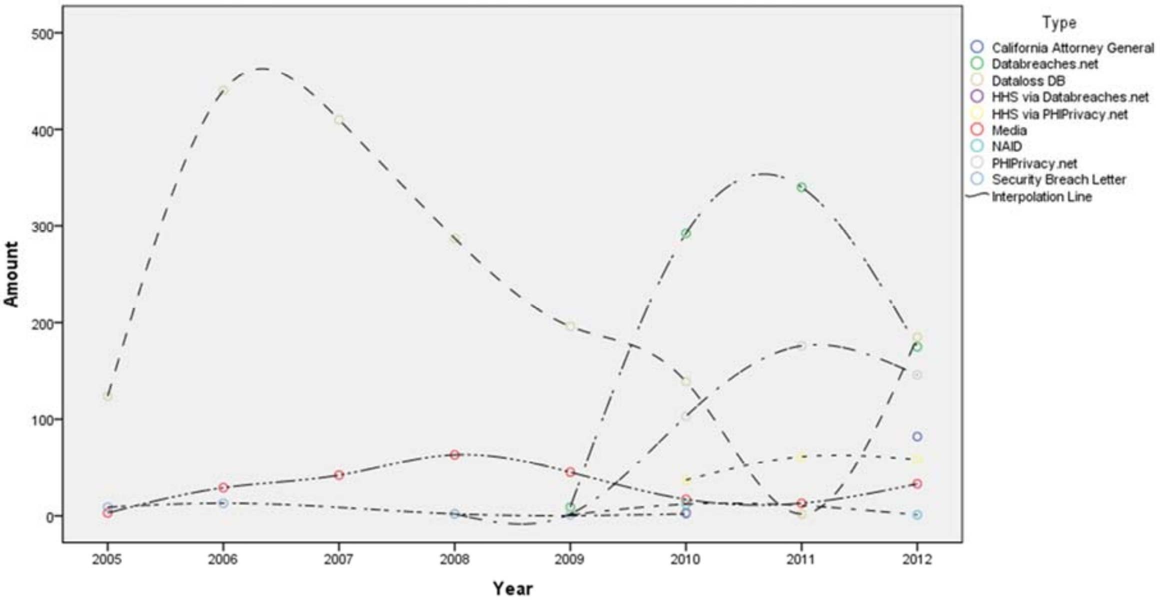


Figure 11: breaches per year per source

After the visualization of the amount of breaches per year and per source the table of the restructured data and the distribution of the amount of breaches per state and per year are displayed.

	2005	2006	2007	2008	2009	2010	2011	2012
Alabama	0	2	6	2	2	2	11	8
Alaska	0	1	1	0	1	2	2	3
Etc.	…	…	…	…	…	…	…	…
Total	133	454	434	345	242	586	554	647

Table 2: visualization of restructured data: Breaches per state per year (all sources)

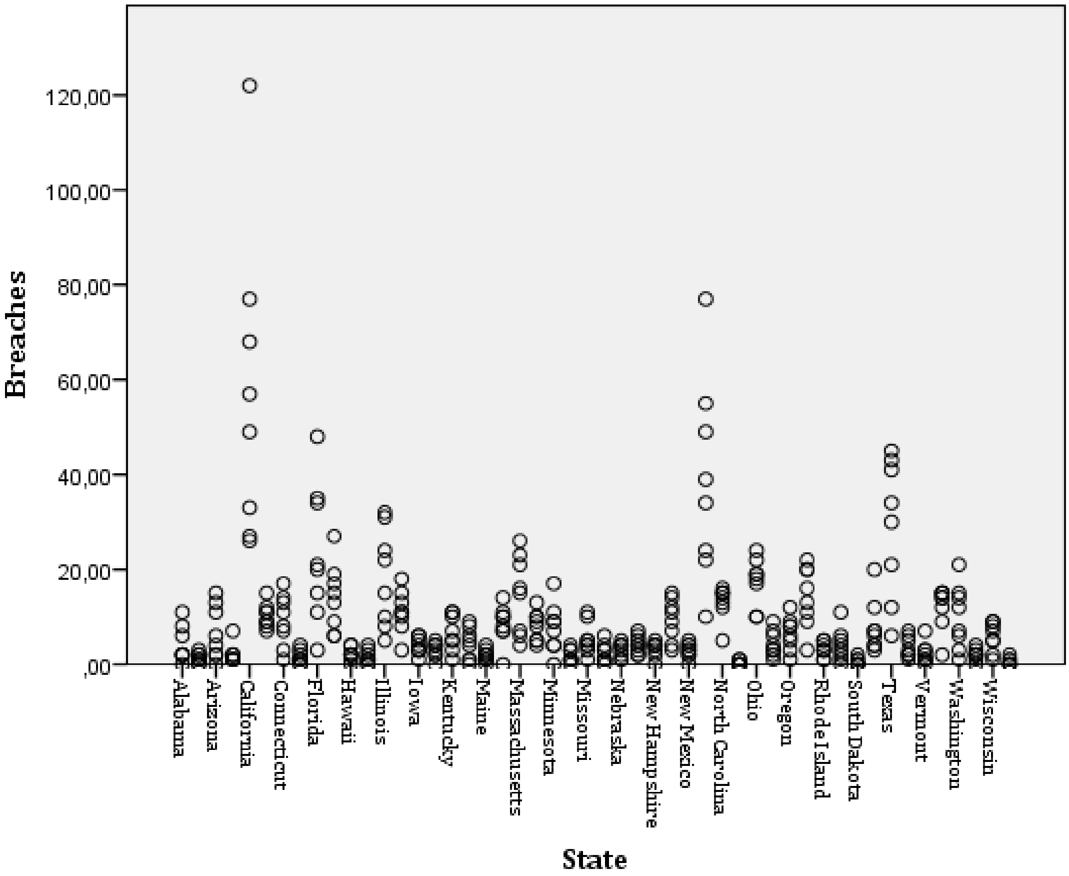


Figure 12: breaches (circle is amount of breaches per year per state; all sources and 50 states included)

The low amount of breaches per state in combination with the low amount of firms represented gives the risk of representative errors, because measurement errors can change the picture of the data in the state. The distribution and the visual inspection of the table with the restructured data shows that most states had between 0 and 20 breaches per year and a few states have a lot more breaches. The average amount of breaches per case is 9 (all sources included).

Apart from these representativeness errors, a few assumptions about the dataset need to be made. The first assumption is that the distribution of the amount of records per breach is equal over all the states. With this assumption, there is no need for taking the wide variation of records into account. In the same way, an equal distribution of the origin of the breaches is assumed. Because it is impossible to exclude third parties and consumers of the database, it is assumed that they are distributed equally among all states. This means that the dataset is in some way representative for the amount of breach notifications coming from firms that fall under an SBNL. Moreover, it is assumed that different sectors respond in a similar manner to security breaches. These assumptions need to be made because the subjects assumed can influence the outcomes of the analysis but cannot be filtered or controlled due to limitations in the model or time constraints. Therefore they will not be tested empirically, but are taken into account while making conclusions about the results of the quantitative analysis.

5.1.4 Variations between states: amount of firms

There are many differences between states that can explain the differences between the amount of breaches per state, for example, criminal activity, the cultural attitude to comply with laws, the GDP, population and Internet percentage rate. The difference between the amounts of breaches per state can possibly also partly be explained by the size of the state. Some states in America such as California and Texas are much larger than others. There are more security breaches reported in larger states because there are more firms that can be breached.[279] A possible controlling variable for this issue could be the amount of firms, because firms make notifications. There are a few large states (for instance, California, Texas and New York), with a lot of firms and many small states with relatively few firms. The amount of firms in a state for each year between 2005 and 2010 is used, which also embodies differences between the amount of firms within a state size over time.[280] A scatter plot of the logarithm of breaches and firms per state shows a visual relationship.

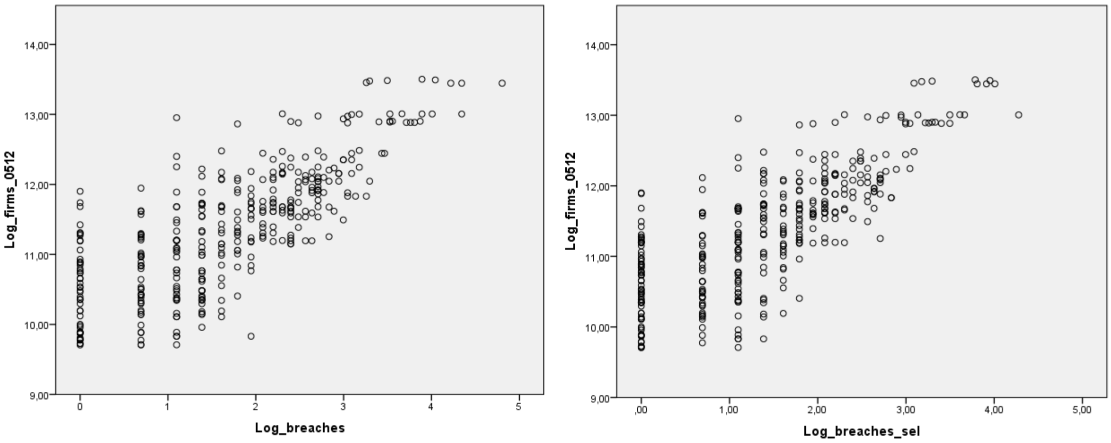


Figure 13: scatterplot of log_breaches and log_firms (Selected sources right)

A correlation analysis shows a significant correlation between the amount of breaches and the amount of firms.

Correlation log *Breaches* and *Firms_per_state*	Coefficient		Significance
	All sources	Selected sources	
Pearson	.805	.832	.000
Spearmans Rho	.771	.777	.000

Table 3: Correlation analysis

When running a standard linear regression, it is shown that the number of firms in a state explains 65% (all sources) or 69% (selected sources) of the variance of the amount of breaches in a state. In a stepwise regression all other control variables (population,

[279] The concentration of vulnerable information technology services, such as in Silicon Valley in California can be another explanation for a higher number of breaches. This variation will not be discussed in this thesis.

[280] 'Firms in U.S. states' (*Census.gov*, 2013) <http://www.census.gov/econ/susb/> accessed 13 June 2013. The amount of firms per state was available up to 2010. Therefore, 2011 and 2012 have 2010 values. The distribution of firm size per state is assumed to be equal.

Internet percentage rate and gdp) are excluded. The visual information, the correlation and regression indicates that breaches can largely be explained by the amount of firms in a state. Therefore, this study controls for this type of variance. In order to do this, the variable *Breaches_per_firm* is constructed: the amount of breaches per state per million firms. The distribution of *Breaches_per_firm* is spread more evenly than *Breaches*. *Breaches_per_firm* will be used as a final dependent variable.

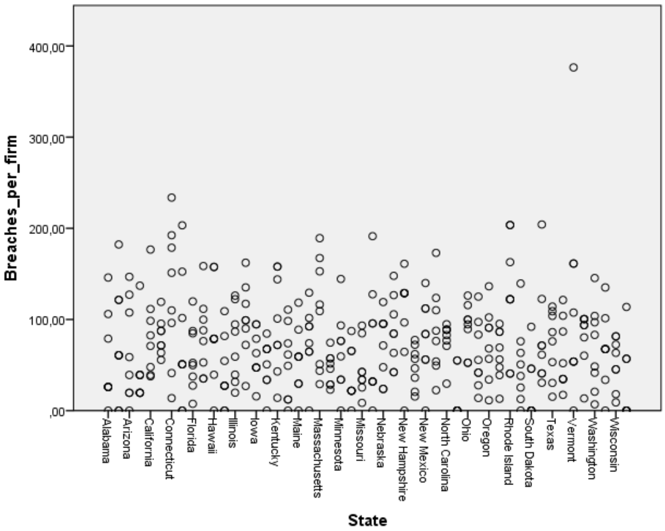


Figure 14: breaches per firm per state (all sources and 50 states included).

5.1.5 Variations over time: Internet security

Just like there are many differences between states, there are also variables that differ over time that can explain the differences of the amount of breaches over time. The particular influence of improved Internet security will be highlighted in this section. Effective notification laws will eventually result in less breach notifications, because the laws improve Internet security.[281] In America, the effect of breach notification laws on Internet security, measured as the amount of identity thefts, is 6.1%, which can be considered quite low.[282] However, this effect, and more particularly its lag time and impact, is not measured for the current dependent variable. Therefore, a rough estimation is performed to get a sense of this effect. To do this, the development of states that had a high number of breaches in the developing period (2005-2008)[283] is compared with countries that had a low number of breaches in the same period. For this analysis, the five states that have the highest amount of breaches per firm in the developing period are grouped. The same is done for firms with a low number of breaches per firm. Both values are compared with the average number of breaches in the mature period (2009-2013).[284] One would expect that a relative high number of reported breaches in the developing period would result in a stronger decrease or less

[281] Ceteris paribus: other factors that influence the amount of notifications over time, such as the activity of cybercriminals resulting in increased Internet insecurity, stay at the same level.

[282] *Ceteris paribus*, see Romanosky (n 255).

[283] In the developing period, only a few states had adopted an SBNL, see section 5.2.1 of this research.

[284] In the mature period, most states had adopted an SBNL, see section 5.2.1 of this research.

increase of notifications with respect to the states with an initial low number of notifications, because of relatively enhanced Internet security. It is assumed that exogenous effect of Internet security develops in the same manner for all states, that breaches have a similar effect on Internet security and that Internet security is equal over states at the beginning of the measurements. The change of breaches over the years in both groups is displayed below for all sources and selected sources[285]

	Average breaches per firm 2005-2008		Average breaches per firm 2009-2012	
	All sources	Selected sources	All sources	Selected sources
Lowest 5 amount of breaches per firm in 2005-2008 (rounded) (Wyoming, North Dakota, Arkansas, Mississippi, Missouri)	75	75	190	120
Highest 5 amount of breaches per firm in 2005-2008 (rounded) (Rhode Island, Connecticut, Ohio, Indiana, Montana)	410	365	425	255

Table 4: positive effects of notifications

The results show that states with a low amount of breaches roughly doubled the amount of breaches that were notified. States that already had a high amount of breaches on average showed a minor increase in the case of all sources and a strong decrease if only the selected sources are taken into account. This absence of notification laws in the states with a low amount of breaches can partly explain a lower amount of notifications in the developing period. Wyoming, Missouri and Mississippi did not have an SBNL from 2005 until 2008 but Arkansas and North Dakota did. States that contained the highest amount of breaches per firm in the developing period all had adopted a law in 2006. But the results could also indicate that, to some extent, a security feedback loop exists. On the other hand, the amount of cases in the data is very low, on average 9 breaches per firm if all the data is included. It is hard to believe that a few breaches have such an impact on Internet security.[286] The negative feedback loop of Internet security therefore is expected to have a certain effect, but a more detailed analysis is needed to analyze this in subsequent research.

5.2 Independent variables: classifications of American SBNLs

The aim of this data analysis is to learn from U.S. data on SBNLs in order to make recommendations for the European and Dutch legislative proposals. This requires the construction of independent variables that contain aspects of an American SBNL. For this purpose, the laws itself and different legal sources from U.S. government institutions and law firms are consulted in order to distinguish and map the different aspects. It would be most desirable to quantify those aspects on an interval/ratio scale,

[285] Selected sources: the dataset that only contains the sources Dataloss DB and Databreaches.net.

[286] However, it could be that more breaches are notified, and that in reality, this number accounts for a large amount of breach notifications.

but this proved to be very difficult, as it is hard to distinguish equal differences between multiple values per aspect. Therefore, several aspects of the law have been classified on dichotomic scale. If the particular law has this aspect, it is classified '1', else '0'.[287]

5.2.1 Introduction date

The introduction date is the first aspect of the law that is mapped.[288] For this purpose, data from the Commercial Law League America (CLLA) is used.[289] This database is an authoritative synthesis of legal analysis, which covers among others the introduction date of American SBNLs and key provisions of the law. The data is updated until December 2011. After this date, no additional adoptions of SBNLs have taken place.

	2005	2006	2007	2008	2009	2010	2011	2012
U.S. States with an SBNL	11	27	36	41	45	45	46	46
	Developing period				Mature period			

Table 5: number of SBNLs per year (out of 50 U.S. States)

Most states adopted an SBNL in the years between 2005 and 2008. This is called the 'developing' period. Between 2009 and 2012 the vast majority of states have a law in place: the 'mature' period. Those periods will be used in the quantitative analysis in chapter 6. It is remarkable that the dataset also contains breaches from years and states that do not have a law. Those are most likely voluntary notifications or notifications from consumers or third parties, but indicate that, contrary to the statements made by the Privacy Breach Clearinghouse, a significant part of the breaches could come from other reporters than the companies affected.

5.2.2 Sanctioning laid down in the law higher than 50000 dollar

The sanction for not complying with the law differs between states. Not complying means not notifying or not notifying in due time or according to the formal requirements demanded. 14 laws can impose a maximum sanction of 50000 dollar or higher. Some states do not predefine a sanction but consider it a task of the Attorney General to impose a sanction, which could possibly be higher than 50000 dollar. The classification *sanctioning* therefore means that there is a predefined penalty of 50000 dollar or higher. These laws are labeled 1. For this classification, a legal analysis that contains aspects of all American SBNLs made by the law firm Mintz Levin has been used. Mintz Levin is a large US law firm with approximately 400 attorneys specialized in privacy and security, which made this chart for information purposes.[290] The

[287] The classifications per state are displayed in appendix B.

[288] Most laws have been amended in some form after their adoption, but most amendments concern an incremental alteration of the laws. Thus, therefore, the introduction date is used for the analysis.

[289] 'Data Breach Notification Laws by State' (*CLLA*, December 2012) <http://www.clla.org/documents/breach.xls> accessed 12 June 2013.

[290] 'State Data Security Breach Notification Laws' (Mintz Levin, 1 December 2012) <http://www.mintz.com/newsletter/2007/PrivSec-DataBreachLaws-02-07/state_data_breach_matrix.pdf> accessed 13 June 2013.

classification is compared with a similar chart of Baker Hostetler, a similar U.S. law firm with 800 attorneys.[291]

5.2.3 Strictness defined by Romanosky

Based on the examination of state laws, Romanosky, a researcher in the field of cybersecurity, highlighted a few states which should be stricter than average after the consultation of attorneys. These are California, Hawaii, Maryland, Massachusetts, Minnesota, Rhode Island, Tennessee, Vermont, and Virginia. Those states all have the following characteristics: "they are acquisition-based (forcing more disclosure from a lower threshold of breach); cover all entities (businesses, data brokers and government institutions); and allow for a private right of action (i.e., individual or class action law suits)."[292]

5.2.4 Individuals have a private right of action

A possible important distinction between the U.S. laws is whether individuals have a private right of action. This means that people injured by a violation of the breach notification may institute a civil action to recover damages. There must however be a relation between the failure to notify and the damages caused. States that have a private right of action are labeled 1. 14 laws allow for a private right of action of individuals. This classification is based on the chart of Baker Hostetler.[293]

5.2.5 Scope of personal information is broader than general definition.

According to Baker Law, the general definition of personal information is "An individual's first name or first initial and last name plus one or more of the following data elements: (i) Social Security Number, (ii) driver's license number or state issued ID card number, (iii), account number, credit card number or debit card number combined with any security code, access code, PIN or password needed to access an account and generally applies to computerized data that includes personal information".[294] Baker law labeled cases with a broader definition of personal data. For example, because medical information a password or a taxpayer identification number is included.[295] Those are labeled 1. 24 laws have a scope of personal information, which is broader than the general definition.

5.2.6 Obligation to notify the Attorney General

A remarkable difference between American laws is the obligation to notify the Attorney General in addition to the person whose data is breached. The Attorney General is a

[291] 'State Data Breach Stature Form' (Baker Hostetler, 2013) <http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/State_Data_Breach_Statute_Form.pdf> accessed 13 June 2013.

[292] Romanosky (n 251) 273; Email with Sasha Romanosky, Research Fellow, Information Law Institute, New York University (9 April 2013).

[293] Baker Hostetler (n 291).

[294] Ibid.

[295] Ibid.

supervising authority and responsible for settling the procedure and potential procedures for damages. 17 of the 50 states require such a notification.[296]

5.2.7 Obligation to notify the customer credit reporting agency

A customer credit reporting agency is "a company that collects information from various sources and provides consumer credit information on individual consumers for a variety of uses. It is an organization providing information on individuals' borrowing and bill-paying habits".[297] A notification to this authority can be required because these agencies maintain and compile personal information files on consumers. 29 laws contain this obligation. In some states, a company only needs to notify a customer credit reporting agency if the amount of records per breach is above 500 or 1000 residents. Laws that have the obligation to notify the customer credit agency, regardless of the threshold, are labeled 1.[298]

5.2.8 Summary

A summary of the independent variables is displayed below. In addition to the independent variables, four control variables have been constructed: the GDP, Internet penetration rate, the number of firms and the population per state.[299]

Description	Label	Number of laws (out of 50)
Maximum sanctioning above $50k	*Sanctioning*	14
Strictness defined by Romanosky	*Strict_Romanosky*	9
Private right of action	*Private_action*	14
Wider scope than the general definition	*Scope_law*	24
Notify Attorney General	*Not_ag*	17
Notify Customer Credit Reporting Agency	*Not_custcredit*	29
GDP per state	*GDPcap_per_state*	Control variable
Internet Penetration rate per state	*Internetpenrate_per_state*	Control variable
Number of firms per state	*Firms_per_state_0512*	Control variable
Population per state	*Pop_per_state*	Control variable

Table 6: summary of the independent variables

[296] Security Breach Notification Chart (Perkins, 2013) <http://www.perkinscoie.com/files/upload/LIT_09_07_SecurityBreachExhibits2.pdf> accessed 4 July 2013.

[297] Arthur O'Sullivan and Steven M. Sheffrin, *Economics: Principles in Action*. (Pearson Prentice Hall 2003), 512.

[298] Perkins (n 296).

[299] 'US GDP' (US Government Revenue, 2013) <http://www.usgovernmentrevenue.com> accessed 13 June 2013; 'Internet penetration rate' (PEW Internet) <http://pewInternet.org/Reports/2012/Digital-differences/Main-Report/Internet-adoption-over-time.aspx> accessed 12 June 2013; 'Firms in U.S. states (n 280); 'Population in U.S. states' (Internet World States, 2013) <http://www.Internetworldstats.com/unitedstates.htm> accessed 12 June 2013.

5.3 Hypotheses

The construction of hypotheses is a last step towards executing the quantitative analysis in the next chapter. In chapter 3, design parameters are distinguished from legal analysis. In chapter 4, relations between aspects of the law and compliance and the amount of notifications are derived from literature. It was assumed that addressees, scope, sanctioning in combination with enforcement are positively related with the amount of breaches. The aim of this chapter was to draw hypotheses in such a way that they also have explanatory power for the Dutch and European situation. Therefore independent variables are clustered to construct hypotheses in the light of the design parameters sanctioning, scope and notification authority. The U.S. laws do not have significant differences in the design parameters addressees and confidential treatment. As such, those two design parameters shall not be tested within this quantitative analysis.

5.3.1 Hypothesis 1: sanctioning

Literature review showed that high sanctions (in combination with strict enforcement) influence the willingness to notify. The independent variables that relate to sanctioning are *Sanctioning*, *Private_action* and *Strict_Romanosky*. Strictness defined by Romanosky also entails elements of scope, and therefore is discussed in the light of hypothesis 2 as well. This hypothesis can be criticized by opposing arguments. For example, the safety culture theory says that people and organizations have to be rewarded instead of punished in order to learn or admit mistakes.[300] The very successful leniency policy in competition law has shown that a mix of high fines and high rewards can incentivize organizations to notify a cartel.[301]

Hypothesis 1a: laws with a **maximum sanctioning above $50k** have a **higher** amount of breaches.
Hypothesis 1b: laws with a **strictness defined by Romanosky** have a **higher** amount of breaches.
Hypothesis 1c: laws with a **private right of action** have a **higher** amount of breaches.

5.3.2 Hypothesis 2: scope

The hypothesis is that a broad breach definition causes more notifications because more cases of breaches fall under the definition of a breach. An opposing argument for this hypothesis is that interviews suggested that if the amount of security breaches that fall under the scope is wide, the willingness to notify would be lower because of a

[300] Patrick Hudson, 'Safety Culture, Theory and Practice' (*Centre for Safety Science, Leiden University.* 1999), 3 <http://ftp.rta.nato.int/public//PubFulltext/RTO/MP/RTO-MP-032///MP-032-08.pdf> accessed 13 June 2013.

[301] European Commission 'Guidelines on the method of setting fines imposed pursuant to Article 23(2)(a) of Regulation No 1/2003 (Leniency Policy)' [2006] OJ L210/02. Organizations that provide information about a cartel in which they participated might receive immunity or reduction from fines.

notification fatigue.[302] The independent variables *Scope* and *Strict_Romanosky* are related to the design parameter scope. The strictness variable defined by Romanosky includes aspects of scope because those laws have a lower threshold for a breach and cover all entities. Therefore strictness defined by Romanosky can also be an indicator for scope.[303]

Hypothesis 2a: laws with a **wider scope than the general definition** have a **higher** amount of breaches.
Hypothesis 2b: laws with a **strictness defined by Romanosky** have a **higher** amount of breaches.

5.3.3 Hypothesis 3: notification authority

Some states require a notification to a notification authority. It is assumed that an obligation to notify the Attorney General or customer credit reporting agency will result in more breaches in the dataset because those agencies are a centrum for data collection. This does not necessarily mean that there are more breaches, but that there are more breaches in the dataset because the notification authority is a central organ for processing this data.

Hypothesis 3a: laws with an **obligation to notify the Attorney General** have a higher amount of breaches.
Hypothesis 3b: laws with an **obligation to notify the Customer Credit Reporting Agency** have a higher amount of breaches.

[302] Interview with Rogier Ragetlie, Security Manager, Brabant Water ('s Hertogenbosch, the Netherlands, 25 April 2013).
[303] It is hard to determine which aspect of the strict laws defined by Romanosky in fact cause any significant result, it could be either relate to sanctioning or scope.

6 Quantitative analysis

This chapter analyses the hypotheses formulated in the former chapter. The effects of an SBNL are expected to be complex and the dataset is flawed. Hence, basic statistical tools such as descriptive analysis and means comparison are a reliable approach. Thus, a descriptive and statistical comparison of the means and medians between the independent variables and the dependent variables is performed. Hereafter, a more advanced statistical model, a fixed effects regression, is executed. A fixed effects regression can control for variations between time and states.[304]

6.1 Comparisons of means and medians

The hypotheses are first tested by comparing the differences between means and medians of the amount of breaches for each classification of the law. Therefore, only cases of breaches in states with an adopted SBNL in that particular year are selected. One cannot measure classifications in the law without the existence of the law. These are 297 cases out of the total of 400 cases. This is an unbalanced panel because laws are not introduced at the same time.[305] Descriptive statistics are displayed for every classification. These are the difference between the average mean and median of *Breaches_per_firm* between the laws that have the aspect that is classified and laws without this aspect.[306] The dataset is observed for three periods: the total timespan (between 2005 and 2012), the developing period (between 2005 and 2008) and the mature period (between 2009 and 2012). An individual year-by-year statistical comparison of means probably would not provide us with much more details, amongst others because that the amount of cases would be too low to make any useful statements. The statistics of the median reflect on the mean results, because outliers of states that have a lot of breaches per firm can blur the picture.

Hereafter, an Independent Samples T-test and Mann-Whitney test are used to analyze whether respectively the means and medians differ significantly. A Mann-Whitney test can in most cases be interpreted as a difference in medians.[307] In most cases, the dependent variable is not normally distributed. In the developing period, the sample size of some observations is lower than 40. An Independent Samples T-test is not allowed in this situation, but the non-parametric Mann-Whitney test is. Before analyzing the classifications, the effect of a law as such, without taking several classifications into account, is analyzed.

[304] An introduction of the fixed effects regression is given in section 1.4.2 of this research.

[305] The panel is unbalanced because laws are adopted at different periods in time. Hence, a different amount of laws are observed for each year in the dataset.

[306] Detailed descriptive statistics can be found in appendix C.

[307] The Mann-Whitney test is not an official comparison of medians, because it compares the mean ranks. There are situations thinkable where a similar median can give a significant outcome for the Mann-Whitney test, if the distributions have a different shape. Because the test is used for a rough analysis in comparison with the samples T-test, these kinds of exceptions will not be taken into account.

6.1.1 Effect of the law

Below the means and medians of *Breaches_per_firm* (and *Breaches_per_firm_sel)* for *Has_law* are displayed.[308] It is clearly visible that there are more notifications in the dataset when the law is adopted.

Database:	All sources				Selected sources			
Value:	0		1		0		1	
Mean/median	Mean	Median	Mean	Median	Mean	Median	Mean	Median
Has_SBNL	77	72	55	50	45	37	37	32

Table 7: descriptive statistics of Has_law (highest marked green)

The mean and median also statistically differ on the .01 level as can be seen in the table below. The values of the means of the selected sources are lower because there are less breaches in the database with the selected sources compared with the database containing all sources.

Has_SBNL	All sources		Selected sources	
	Parametric	Mann-Whitney	Parametric	Mann-Whitney
2005-2012 (total)	.000	.000	.000	.000

Table 8: comparison of means and medians of the Has_law classification

6.1.2 Testing hypothesis 1

Below the means and medians of *Breaches_per_firm* for the classifications related to sanctioning are displayed. The means and medians of each classification *per year* is displayed in appendix C.

Database:	All sources				Selected sources			
Value:	0		1		0		1	
Mean/median	Mean	Median	Mean	Median	Mean	Median	Mean	Median
Sanctioning	78	72	75	75	56	47	54	53
Strict_Romanosky	72	68	99	92	51	48	72	65
Private_action	73	66	86	89	53	47	61	60

Table 9: descriptive statistics of sanctioning related classifications (highest marked green)

The descriptive analysis shows that the highest mean of *Sanctioning* lies at the states labeled 0, while the states that are labeled 1 have the highest median. Besides, the differences are very small. This suggests that the classification *Sanctioning* does not generate a lot of differences in the amount of breaches in the database. *Strict_Romanosky* and *Private_action* have higher means and medians for states labeled 1. This direction corresponds with hypothesis 1b and 1c. The dataset that includes all sources does not show a different pattern than the dataset with selected sources. The following bar chart of *Strict_Romanosky* is based on the data in Appendix C. Laws that are stricter according to Romanosky have a higher mean and median compared to the laws that do not have such a strictness, except for the median of 2007 and 2012.

[308] Values are rounded.

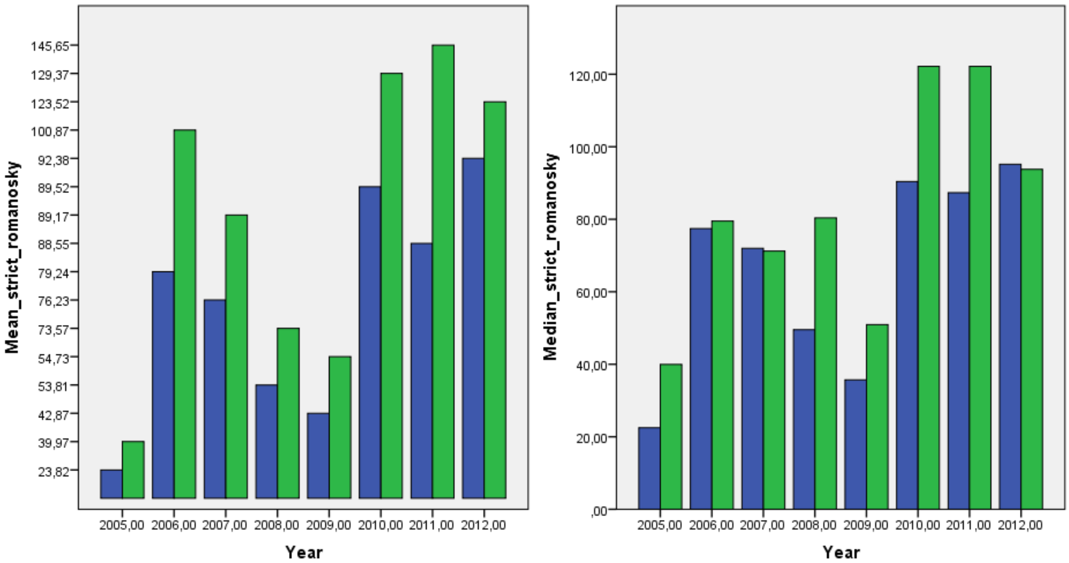


Figure 1: bar of strict_Romanosky (all sources, green is one, left median, right mean)

The next analysis is a comparison of those means and medians using a parametric Independent Samples T-test and a non-parametric Mann-Whitney test. A comparison of all the cases covering all the years of data collection has been performed. As said, separate comparisons of means and medians are executed in order to analyze differences between the developing period and the mature period. The results are shown below.[309]

Sanctioning	All sources		Selected sources	
	Parametric	Mann-Whitney	Parametric	Mann-Whitney
2005-2012 (total)	.510	.916	.616	.582
2005-2008 (n=31)	.939	.910	.765	.965
2009-2012	.329	.774	.729	.464
Strict_Romanosky				
	Parametric	Mann-Whitney	Parametric	Mann-Whitney
2005-2012 (total)	.003	.002	.002	.001
2005-2008 (n=21)	.169	.138	.133	.085
2009-2012	.007	.003	.008	.007
Private_action				
	Parametric	Mann-Whitney	Parametric	Mann-Whitney
2005-2012 (total)	.039	.006	.115	.017
2005-2008 (n=30)	.618	.267	.289	.077
2009-2012	.049	.012	.232	.096

Table 10: comparison of means and medians of sanctioning related classifications (significant results marked green)

The results show that there are significant differences between means and medians on the 0,01 level for *Strict_Romanosky* for the total group and the mature period. The mature period contains more cases, thus is more likely to influence the total picture, which could explain the similarities in results. *Private_action* shows a similar pattern for

[309] A low number of cases (n>60) is mentioned. All other observation have a higher number of cases.

all the sources, but does not produces significant results for selected sources except for the Mann-Whitney test. The fact that there are no differences in the developing phase could be attributed to the fact that most (aspects of the) laws need a certain period to become effective and that real impact can only be observed after a couple of years.

6.1.3 Testing hypothesis 2

Database:	All sources				Selected sources			
Value:	0		1		0		1	
Mean/median	Mean	Median	Mean	Median	Mean	Median	Mean	Median
Scope_law	77	71	77	74	54	48	56	52
Strict_Romanosky	72	68	99	92	51	48	72	65

Table 11: descriptive statistics of scope related classifications (highest marked green)

The descriptive analysis of the classifications related to hypothesis 2 shows that laws with a wider scope have slightly more breaches per firm for the selected sources. This is however not confirmed by the database with all sources. This database shows a mixed pattern, which indicates no significant difference. The independent variable *Strict_Romanosky* differs significantly.[310]

Scope_law	All sources		Selected sources	
	Parametric	Mann-Whitney	Parametric	Mann-Whitney
2005-2012 (total)	.944	.910	.727	.588
2005-2008 (n=49)	.522	.786	.827	.777
2009-2012	.879	.945	.516	.670
Strict_Romanosky				
	Parametric	Mann-Whitney	Parametric	Mann-Whitney
2005-2012 (total)	.003	.002	.002	.001
2005-2008 (n=21)	~~.169~~	.138	~~.133~~	.085
2009-2012	.007	.003	.008	.007

Table 12: comparison of means and medians of scope related classifications (significant results marked green)

The comparison of means and medians shows no significant difference for scope. This was expected from the descriptive statistics. *Strict_Romanosky* contains both elements of scope and sanctioning. The question is whether the scope or the sanctioning aspect of *Strict_Romanosky* would determine the significant difference. Based on this data, it is more likely that its sanctioning aspect will explain the higher amount of breaches for laws that are strict according to Romanosky, because *Private_action* shows similar results.

6.1.4 Testing hypothesis 3

Hypothesis 3 shows a major difference between the means and medians of the laws that do have the classifications *Not_ag* and *Not_custcredit* and the laws without this classification.

[310] As already discussed in section 6.1.2 of this research.

Database:	All sources				Selected sources			
Value:	0		1		0		1	
Mean/median	Mean	Median	Mean	Median	Mean	Median	Mean	Median
Not_ag	71	67	88	84	50	47	65	60
Not_custcredit	70	56	82	78	48	41	60	53

Table 13: descriptive statistics of notification authority related classifications (highest marked green)

The descriptive statistics of *Not_ag* and *Not_custcredit* show results that correspond with the hypotheses. There are, on average, more breaches if these obligations are present in the law.

Not_ag	All sources		Selected sources	
	Parametric	Mann-Whitney	Parametric	Mann-Whitney
2005-2012 (total)	.004	.009	.001	.001
2005-2008 (n=39)	~~.091~~	.063	~~.076~~	.041
2009-2012	.024	.066	.005	.014
Not_custcredit				
	Parametric	Mann-Whitney	Parametric	Mann-Whitney
2005-2012 (total)	.044	.016	.010	.002
2005-2008 (n=48)	.209	.032	.109	.011
2009-2012	.159	.199	.042	.054

Table 14: comparison of means and medians of notification authority related classifications (significant results marked green)

The parametric t-test and Mann-Whitney test show that both classifications render significant differences for the whole time span. The obligation to notify the Attorney General is even significant at the .01 level. The picture is less clear for the developing and mature period.

6.2 Fixed effects regression

The comparison of means has some major drawbacks, which can partly be solved by a fixed effects regression model. The comparison of means is vulnerable for differences in the amounts of breach notifications between states that are not caused by the differences between laws, but by other variables that are omitted from the analysis. The analysis is also vulnerable for effects over time, such as the effect of Internet security. Section 5.1.4 discussed for variables that differ between states and controlled for the amount of firms per year by dividing the number of notifications by the amount of firms. However, there are still many variables that differ between states that are not discussed. Section 5.1.5 discussed the negative feedback effect of Internet security that changes over time, which is an omitted variable from the analysis. It is impossible to control for all variables that vary over time or between states, because it is impossible to identify all possible variables and to categorize them in a quantitative manner. Moreover, the comparison of means indicates rough relations between the dichotomous independent variables and the dependent variable. A statistical model can improve the interpretation of the correlations. A possible solution for the problem of omitted variables is the fixed effects regression model, a standard econometric tool that is used for longitudinal data.[311] The mechanism of the fixed effects regression method has been explained briefly in section 1.4.3.

6.2.1 The model

Two models have been used to capture the impact of the classifications of the law on the amount of breaches per firm. The first model does not take the adoption of the law into account; it focuses entirely on the impact of the classifications of the law for the moment that states had adopted the law. This results in an unbalanced panel.[312] To acquire a somewhat more reliable balanced panel, the breaches that were collected without the existence of a law are entered into the model as well.[313] For this purpose, the variable *Has_law* is used and interacted with the classifications of the law. The model is reconstructed for the independent variables that turned out to be significant.

Model 1: unbalanced panel (297 cases)

$$\textit{Breaches\_per\_firm(\_sel)} = \beta_0 + \beta_{\text{Sanctioning}} + \beta_{\text{Strict\_Romanosky}} + \beta_{\text{Private\_action}} + \beta_{\text{Scope\_law}} + \beta_{\text{Not\_ag}} + \beta_{\text{Not\_custcredit}} + \gamma_s + \delta_t + \varepsilon_s$$

Model 2: balanced panel with *Has_SBNL* (400 cases)

$$\textit{Breaches\_per\_firm(\_sel)} = \beta_0 + \beta_{\text{Has\_SBNL}} + \beta_{\text{Has\_SBNL}} {}^{*} (\beta_{\text{Sanctioning}} + \beta_{\text{Strict\_Romanosky}} + \beta_{\text{Private\_action}} + \beta_{\text{Scope\_law}} + \beta_{\text{Not\_ag}}\ \beta_{\text{Not\_custcredit}}) + \gamma_s + \delta_t + \varepsilon_s$$

Alternative dependent variables

Breaches_per_firm_sel / *Log_breaches* / *Log_breaches_sel*

The independent variables are dummy variables. γ_s, δ_t and ε_s are respectively state fixed effects, time fixed effects and the error term.[314] As said, the fixed effects model is able to take correlations between several years of a law into account. This requires an assumption about the structure of the correlations between occasions. This called the covariance structure.[315] Out of many types of covariance structures, the autoregressive and compound symmetry functions are the best candidates to fit the data.[316] The autoregressive structure is the most commonly used structure in these kinds of fixed effect regression and therefore used in the model.[317] The model below displays the

[311] Interview with Thijs Urlings, Assistent Professor, Innovation and Public Sector Efficiency, Delft University of Technology (Delft, the Netherlands, 3 May 2013).

[312] The panel is unbalanced because laws are adopted at different periods in time. Hence, a different amount of laws are observed for each year in the dataset.

[313] Ibid.

[314] Verbeek (n 84) 345-347.

[315] Ronald H. Heck, *Multilevel and Longitudinal Modeling with IBM SPSS* (Routledge, 2010) 163, 164.

[316] Compound symmetry assumes equal variances and equal covariances across occasions that are constant over time. The autoregressive covariance structure assumes that the residual covariances between measurement occasions within subjects (=states) are correlated but decline exponentially with the distance. Hence, these structures are fairly similar.

[317] Chuck Kincaid 'Guidelines for Selecting the Covariance Structure in Mixed Model Analysis' (*SUGI*, 10 April 2005) 30 <http://www2.sas.com/proceedings/sugi30/198-30.pdf> accessed 13 June 2013.

coefficients and significance of the independent variables. The SPSS mixed models procedure does not produce an R-squared statistic, because "definitions for an R-square for become problematic in models with multiple error terms", caused by the multiple measurements.[318] Each model is repeated for the independent variables that were significant in the model. This iteration is displayed after the slash.

Independent variables (effect for = 0)	*Breaches_per_firm* [First run]/[Repeated]		*Breaches_per_firm_sel* [First run]/[Repeated]	
	Balanced	Unbalanced	Balanced	Unbalanced
Has_SBNL	-41.7***/-79.6***	Not analyzed	-20.3/-37.4***	Not analyzed
Sanctioning	-	-	-	-
Strict_Romanosky	-17.3** /-28.5***	-18.5*/-28.4***	-12.5*/-20.4***	-13.1*/-16.8***
Private_action	-	-	-	-
Scope_law	-	-	-	-
Not_ag	-	-	-	-12.0**/-9.8*
Not_custcredit	-	-	-	-10.9**/-
Constant	95.3***/95.9***	96.6***/97.1***	68.9***/68.9***	69.5***/75.5***
Observations	400	297	400	297
Number of states	46	50	46	50
Significance: *** p<.01; **p<.05; p<.1; '-'p>.1				

Table 15: results of the fixed effects regression model

The results partly confirm the insights from the comparison of means but also display differences. The adoption of a law does have a significant effect on the amount of breach notifications, as expected. This confirms the significant differences in means and medians that were found in section 6.1. The absence of a law results in a reduction between on average 79.6/95.9=83% and 37.4/68.9=54%. *Strict_Romanosky* has a significant impact on the amount of breaches per million firms in a state just as in section 6.1.2. The coefficients reflect the effect for the *absence* of the classification, which is with label '0'. Therefore, the parameters in the model have an opposite sign. Hence, states that are not labeled 1 for *Strict_romanosky* perform worse regarding the amount of breaches. It is notable that their relative impact is almost exactly the same for the database with all sources and selected sources. The absence of *Strict_romanosky* laws reduces the intercept with 28.5/95.9=29.7% for all sources and selected sources 20.4/68.9=29.6%. Both *Sanctioning* and *Scope_law* do not have a significant impact in the model. This also corresponds with the findings in the comparison of means. But, *Private_action*, *Not_ag* and *Not_custcredit*, which partly had significant results concerning the means comparison, are not significant in this model except for *Not_ag* in the unbalanced selected sources dataset.[319] This can be caused by the fact that states

[318] 'R-square statistics in SPSS Mixed Models' (*IBM support*, 9 July 2011) <http://www-01.ibm.com/support/docview.wss?uid=swg21481012> accessed 13 June 2013.

[319] Except for the unbalanced model with selected sources, but this only results in *Not_ag* being significant on the 0.1 level, which cannot be regarded as a powerful result.

with these laws already had a higher amount of breaches at the start of the measurements, which cannot be attributed to this particular aspect of the law. Contrary to the comparison of means, the fixed effects regression controls for these kinds of errors. Furthermore, the balanced and unbalanced panels and the database with all sources and the database with selected sources perform quite similar.

6.2.2 Robustness check

Robustness checks have already been made by constructing both a balanced panel and an unbalanced panel, and by running the model for both the dataset that includes all sources and the dataset that only includes selected sources. In addition to that, the dependent variable is transformed to the logarithmic transformation of the amount of breaches, thus without dividing by the number of firms. The logarithmic transformation of the number of firms is used as a control variable in the model, because this variable varies between states and over time and cannot be filtered by the fixed effects regression. The outcome for the alternative model is displayed below:

Dependent variable (effect for = 0)	*Log_breaches*		*Log_breaches_sel*	
	Balanced	Unbalanced	Balanced	Unbalanced
Has_SBNL	-/.86***	Not analyzed	-/-.58***	Not analyzed
Sanctioning	-	-	-	-
Strict_Romanosky	-.25*/-.33*	-.26**/-.34***	-.22**/-.24**	-.22**/-.25**
Private_action	-	-	-	-
Scope_law	-	-	-	-
Not_ag	-	-	-.20**/.19**	-.19**/-.18**
Not_custcredit	-.16*/-	-.16*	-	-
Log_firms0512	.88***/.88***	.92***/.92***	.85***/.86***	.89***/.87***
Significance: *** p<.01; **p<.05; p<.1; '-'p>.1				

Table 16: robustness check fixed effects regression

Mainly *Strict_Romanosky* is able to hold the robustness check, being significant at on average the .05 level. It is not surprisingly that the number of firms is highly significant. This corresponds with the high correlations found in section 6.1.1. *Not_ag* produces some significant results at the .05% level for the dataset with the selected breaches. Hence, *Not_ag* is fairly robust on the unbalanced selected sources model.

6.3 Verification & validation of the quantitative analysis

6.3.1 Verification

The analysis has various limitations, which are partly tackled by the approach followed. First, the representativeness of the dataset is hampered. The amount of breaches per case is relatively low. In addition to that, the dataset is constructed out of multiple sources that are not mutually exclusive and representative. Those limitations have been discussed in chapter 5. In order to tackle the latter problem, the dataset has been run separately for two relative representative selected sources. In addition to this, fixed effects regression, a sophisticated statistical tool, requires complete data. Given the list of assumptions and the low representativeness of the dataset, there is a risk of over-interpreting the results.

Second, there are multiple inherently omitted variables that can change over time and between states. In the means comparison, this limitation is mitigated by separating a developing and a mature period and by controlling for the number of firms in a state. This issue is treated more thoroughly in the fixed effect regression. This method controls for state and time differences. However, the fixed effects regression does not control for variables that differ between states and over time simultaneously. For example, Internet security can vary between states but also over time. The results thus should be treated with care. However, the results that have proven to be robust are expected to explain the effects of American SBNLs.

6.3.2 Validation

The aim of this chapter was to learn from the available American data in order to make recommendations for the European and Dutch legislative proposals. Applying insights of the American quantitative analysis and the structure of American laws to the other side of the Atlantic is a question of legal transplantation.[320] Laws have been transplanted since the Roman ages, at the time of the codex Justinianus.[321] Nowadays, globalization and the availability of information increased the speed of legal transplantation. A corner stone concept of legal transplantation is that the law and its effects probably better fits if it stands alone from the local culture.

The performed quantitative analysis of the American situation has (some) external validity for the European Union. The American laws have more similarities with the European PDPR than the PCD. The American laws and the PDPR focus on the protection of personal data and both can impose heavy sanctions. But still, there are also major differences. For instance, the claim culture in the United States differs from the European Union. Companies in the U.S. are possibly more receptive for high sanctions in the U.S and will notify earlier.[322] Thus, there are specific cultural elements embedded in the results of American data analysis. On the other hand, the cross border effect and universality of the Internet and Internet insecurity suggests that the data analysis can be transplanted to the European situation to some extent.

6.4 Conclusions

The aim of this chapter was to test the hypotheses formed in the former chapter. The present data is not ideal, but nevertheless there are conclusions to make about the effects of an SBNL on the amount of breaches in the dataset. Several analyses for (multiple intersections of) the dataset have been made. The conclusions depend on how strict one wants to interpret the results.

[320] Alan Watson, *Legal Transplants, An Approach to Comparative Law* (Second Edition, University of Georgia Press, 1994).

[321] Martin de Jong, Konstantinos Lalenis and Virginie Mamadouh, *The Theory and Practice of Institutional Transplantation* (Kluwer, 2002), 281.

[322] Interview by email with Arnoud Engelfriet, Associate at ICTrecht (3 May 2013).

First, the adoption of a law clearly relates to more security breaches in the database. This is confirmed by both the means comparison and the fixed effects regression. The absence of an SBNL results in on average between 83% en 54% decrease of the amount of security breaches in the database. The database is partly constructed by underlying sources that only register officially notified breaches, which can explain this high relative increase.

Second, the laws that are defined strict by Romanosky are quite undisputedly related with a higher number of breaches, both in the fixed effects regression and the comparison of means.[323] The explanation for this would lie in the fact that the adoption of a law caused security breach notifications to flow into the notification system and that stricter laws give more rational incentives for compliance. Unfortunately, the underlying effect of the variable strictness is less clear, because it consists of multiple characteristics.

Third, there are independent variables that did not stand the entire statistical procedure. It could be doubted whether these classifications of the law have an effect. Laws that allowed for a private right of action or had an obligation to notify the Attorney General or the Customer Credit Reporting Agency were positively associated with higher laws in the comparison of means, but could not stand the fixed regression test.

Fourth, it is clear that laws with a sanction higher than 50000 dollar and a wider scope than the general definition do not differ in the amount of notifications compared with laws that did not have those properties. Hence, this is an clear rejection of the hypothesis that high sanctions or a broad scope do have an effect on compliance. However, this rejection can partly be attributed to way this these design parameters are constructed. Within *Sanctioning* for instance, laws with sanction higher than 50000 dollar are separated from laws that did not impose such a sanction. However, some laws do not have a predefined sanction, but these laws potentially leave open the possibility to impose sanctions above 50000 dollar. Moreover, some laws also allow for private right of action, which can increase the total 'sanction' that can be imposed, which is not included in this variable, but in the separate *Private_action* variable.

[323] Because "they are acquisition-based (forcing more disclosure from a lower threshold of breach); cover all entities (businesses, data brokers and government institutions); and allow for a private right of action (i.e., individual or class action law suits)" (Romanosky (n 255) 273).

7 Qualitative analysis

The qualitative analysis reviews the perception of Dutch security experts and managers regarding the first and second order effect and outcomes of the quantitative analysis. First, the respondents are asked for the effects of SBNLs. Second, the results of literature review and quantitative analysis are presented and discussed. Third, the respondents have reflected on the approach of measuring effectiveness in the quantitative analysis. Fourth, the respondents also reviewed the proposed Dutch and European SBNLs

7.1 Experts interviewed

Two types of respondents have been interviewed: information security experts and security managers of companies with a complex computer defense system. Because the quality of the analysis strongly depends on the knowledge of the respondents related to the specific theme the following list of criteria is applied to select them.

1.) The respondent must have extensive experience in Internet security and/or Internet law. (10 year+ or recently educated).
2.) The respondent must possess a key Internet security and/or Internet law related position.
3.) The respondent must have knowledge about SBNLs.

Based on these three criteria the following respondents are selected, as is represented in the table below. As said, a distinction is made between experts and security managers.

Name	Position	Type	Interview duration
Mr. R. Prins	Director and founder at Fox IT (a cybersecurity consultancy company)	Expert	1h
Mr. R. Ragetlie	Risk manager at Brabant Water (a water utility company)	Security manager	1h
Mr. A. Engelfriet	Associate at ICTrecht (a legal ICT consultancy company)	Expert	(interview by email)
Mr. W. Vrijssen	Chief Technology Security Officer at Vodafone (a telecommunications provider)	Security manager	1h

Table 17: list of respondents

Both Vodafone and Brabant Water fall under the Dutch SBNL initiative. In addition to that, Vodafone has to comply with the Dutch implementation of the E-privacy Directive, which is the predecessor of the proposal for a general SBNL in the PDPR.[324] The security

[324] Article 4(2) of Directive 2009/136/EC; Article 11.3a Telecommunicatiewet (Telecommunication law).

managers can thus generate insights on their perception of the Dutch and the European initiative.

7.2 Results

First, the perception of incentives for compliance of respondents is displayed. Second, the respondents reflected on the quantitative analysis and the dataset. Third, the respondents have generated expectations on the second order effect of SBNLs.

7.2.1 First order effect

The consideration for compliance is mainly perceived as a cost benefit analysis, although the experts interviewed also mention social responsibility as an incentive to comply with SBNLs. The security managers stated that they would comply with the law voluntarily, according to the logic of appropriateness. The experts confirmed that, probably, a part of the companies would comply voluntary. However, if a company believes that the avoidance of fines is possible, they have a strong incentive to fix the leak internally without disclosure. One expert notes that it is unlikely that there are a lot of voluntary notifications in the United States, because of the claim culture that exists.

The concurring opinion of all the respondents is that high sanctions in combination with strict enforcement will provide the most important incentive for compliance. As one respondent puts it, a risk to get imposed a fine of possibly 2% of the turnover of a company [in the European situation] "will be discussed on board level". Respondents mentioned enforcement of sanctions as an important driver for compliance, for example in the form of security audits. A security manager had experience with friendly audits of the supervisor concerned with the SBNL in the telecommunication sector and perceived this audit positively because it caused increased awareness of security at employees and the optimizations of security processes. Another expert put forward an example of Dutch consumer law to demonstrate the effect of enforcement. Compliance in Dutch consumer law increased according to this expert after the supervisory authority concerned actually imposed fines.

It is confirmed by all the respondents that reputation damage is a major incentive for non-compliance. The publication of the imposition of the sanction in the media is also expected to have an additional negative reputational impact. The respondents however also note that major security breaches have large likelihood of being published in the media beyond the control of a company. A security manager imposes the hypothesis that small breaches will not be notified and that large breaches will be notified. Large security breaches are regarded to have a high likelihood to be published in the media.

7.2.2 Reflection on quantitative analysis and the dataset

The respondents formed the following opinions on the effects of the independent variables of the quantitative analysis. The independent variable *sanctioning* is expected to have the most impact on the amount of notifications, which contradicts the observations in the quantitative analysis. Some respondents also expect a *private action* possibility to have an effect. However, there is a risk perceived that companies are not able to respond to major claims and go bankruptk, which is not beneficial for the system. An increased *scope* is expected to increase the amount of breaches.

The respondents identified several problems with measuring effects in the quantitative analysis, which places the observations into perspective. The fact that it is unknown how many companies are non-compliant is mentioned frequently as a barrier to valuing the number of compliant companies. Moreover, the term breach is questioned as a proxy to measure effectiveness, as there are multiple variables that influence the number of breach notifications. The number of breaches is expected to decline if the SBNL has a positive effect on Internet security or because criminals shift their businesses. Moreover, a breach does not contain information about its severity and the extent to which a company lost control.

All the respondents explain the representation of 0.05% of the American companies in the dataset by both incompleteness and non-compliance of companies. According to the respondents, a multiple of the American companies must have perceived a loss of personal data between 2005 and 2012. The idea perceived by all respondents is that cybercrime is daily business and that the main characteristic of cyberthreats is its universality in being a threat for all types of businesses.

The respondents list several attributes of a breach that have to be processed in a database to make an enhanced analysis for future research. These involve the characteristics of the data theft and the amounts of personal data that are stolen. Moreover, it is important to know whether there is damage or potential damage if integrity is lost. Overall, respondents are interested in detailed description about how the breach occurred and the industry in which the breached took place.

7.2.3 Second order effect

Experts regard insights in the scope of the Internet security problem and its negative effects on society as a positive effect. Moreover, respondents perceive that an SBNL generates an incentive for organizations to increase security practices in order to avoid reputational damage (see also the sunlight as disinfectant mechanism, discussed in section 4.2.). The possible assistance of a capable government that assists in mitigating losses after a security breach is also perceived as positive effect.

An expert notes that an SBNL possibly has a negative effect on Internet security because the focus of the SBNL lies on the notification of breaches and not on the improvement of security as such. He proposes a sanction on bad security practices itself instead of non-compliance with a notification law. Another expert states that the juridification of the problem can be a potential threat. The administrative burden to comply with the law is also perceived as a negative effect.

7.2.4 Review of the Dutch initiative, the PDPR and the PCD

Both experts as well as security managers noted that clear and not too broad legislation are preferred. The security managers discussed the 'vaguely defined' criterion of societal shock of the Dutch initiative.[325] According to them, a loss of integrity "must be a deviation from the normal situation". Hence, the 'significance' of a significant loss of integrity breach in Article 14 PCD must be clearly defined. The obligation to notify insignificant security breaches is perceived to create an unnecessary administrative burden for companies. Security experts urge to include both the loss of integrity as well as the loss of personal data in the definition of a breach.

If the government wants to impose an obligation to notify security breaches, they must have substantive expertise in mitigating losses and exchange information. But, security managers do not regard the current role of the (Dutch) government as a center for information exchange and control as effective. The government, for example, currently does not share information about personal data breaches in the telecommunication sector. In addition to that, the government is inert in processing the information gained from the security breach notifications into useful strategies. Moreover, there are doubts concerning the technical expertise of the government.

Security managers perceive confidential treatment as a minor incentive. This is partly attributed to the fact that public disclosure requests can render a confidential treatment incompatible in the Netherlands. Experts perceive a relationship of trust with the supervisory authority possibly as an incentive for compliance with the law. A part of this relationship is the assistance of the supervisory authority. It is hard to establish a relationship of trust if the supervisory authority also is responsible for the imposition of sanctions. A security manager noted that a relationship of trust between competitors is of much more importance to stimulate information exchange than a degree of trust with the supervisory authority.

The Dutch initiative and the PCD do not impose sanctions. Moreover, there is ambiguity about the scope of 'societal shock' and 'significance' respectively.[326] Furthermore, the respondents perceived limited auxiliary potential of the Dutch government and the European Union. This provides the image of a law that is potentially ineffective. As one expert puts it: "one does not need a law that contains an obligation to notify the fire department if your house is on fire". He meant that voluntary compliance would only exist when a notification is beneficial for the company that notifies.

The sanctions of the PDPR are expected to provide incentives for compliance. Enforcement of a breach is important in this respect. A disadvantage of the PDPR is its broad scope. The PDPR covers all kinds of personal data that can impose an unnecessary administrative burden on companies.[327] The absence of a loss of integrity breach obligation causes important breaches to fall outside the scope of the law.

[325] See section 3.2.3 of this research.
[326] See section 3.3.3 of this research.
[327] Ibid.

7.3 Conclusions

The respondents regard that both the logic of consequences and the logic of appropriateness plays a role in incentivizing companies to comply with the law. The logic of consequences is regarded as the strongest driver. According to the respondents, the main cost benefit decision is to balance enforced sanctions with expected reputation damage.

It is interesting to see that the interviewed security officers of the companies do not see any problems to comply with the law for their own company, but do estimate that a lot of companies will not comply because of possible reputation damage. The implication of this is that the real behavior of organizations to make a notification consideration is not entirely revealed.

The second order effects associated with SBNLs largely correspond with effects distinguished in literature.

Part γ: synthesis and conclusions

- In part γ, the results of the three types of analysis of part β are synthesized.
- This results in a conceptual framework and a comparison of the effects analyzed in part β with the aims of the legislation, analyzed in part α.
- Hereafter, the conclusions and recommendations of the research are presented.

8 Synthesis of literature review, quantitative & qualitative analysis & the aims of legislation

Chapter 4 concerned effects in literature, chapter 5 & 6 concerned effects in American data and chapter 7 concerned the perception of effects by Dutch security experts and managers. This chapter will place the three perspectives on effects of SBNLs in conjunction with each other. As a result of this synthesis, a framework is introduced that aims to give an overview of the mechanisms relating to the first order effect of an SBNL. Apart from this, the effects are compared with the aims of the legislation.

8.1 First order effect

Literature research showed that there are various incentives for compliance with SBNLs. Reputation damage affects compliance negatively. Sanctioning, benefits of information sharing, appropriateness of the law confidential treatment by the notification authority affect compliance positively.

The experts and security managers in the qualitative analysis distinguish the same incentives for compliance as identified in literature. The added value of the qualitative analysis is twofold. First, the qualitative analysis can give an indication of the relative importance of the incentives in literature. Second, the qualitative analysis can reflect on the results found in the quantitative analysis and the methods applied to measure effectiveness. The qualitative analysis shows the importance of sanctions and reputation damage. Confidential treatment by the notification authority, if applicable, is not perceived as a major driver for compliance. Benefits of information sharing are also not perceived as a major driver to comply. Voluntary compliance, according to the logic of appropriateness on the other hand is perceived as a major driver.

The first order effect has been proved empirically by American data in this study. The laws have an effect on the amount of breach notifications. The effect is relatively large: a notification increase of at least 50% can be attributed to the law by a fixed effects regression analyzing differences in breach notification before and after the introduction of the law. The database is partly constructed by underlying sources that only register officially notified breaches, which can explain this high relative increase. From an absolute perspective, the effect is minor: less than 0.05% of the companies notified a security breach in America in the eight-year period that was researched. To compare: A recent study in the United Kingdom published that 88% of the companies searched had experienced data theft in 2009. The low absolute effect could be explained by the incompleteness of the dataset, high compliance costs for a company due to reputation damage and unawareness of breaches. The adoption of the law thus has a structural first order effect, at least in the database of know security breaches. It is however ambiguous which aspects of the law provide this effect. Literature and qualitative analysis showed that enforced sanctions generate compliance with the law and that reputation damage is a major driver for non-compliance. Confidential treatment of the notification and benefits from information sharing about security breaches are perceived as minor incentives for compliance. The quantitative analysis only confirmed that some American laws qualified as strict by American Attorneys cause an increase in notifications, but it is ambiguous what exactly makes these laws strict.

The expected effect of high sanctions in literature and qualitative analysis is not confirmed in the quantitative analysis. Although, the variable *sanctioning* is not a perfect proxy for enforced sanctions, there was no difference observed for the amount of notifications for laws with high sanctions and laws without. This can be explained by the fact that, even in the case of high sanctions, the cost of compliance is still higher than the cost of non-compliance, because reputational damage is high. An alternative explanation for the absence of the effect of sanctions is that sanctions are not an important driver for compliance, contrary to the views in literature and expert interviews. This would be unlikely, since sanctions are regarded as one of the most important drivers for compliance.

The results of the quantitative analysis are interpreted conservatively. If one would only take the comparison of means into account for drawing conclusions, a private action possibility and obligations to notify the Attorney General and customer credit report would positively affect the number of breaches in the database. This is also supported to some extend in the fixed effects regression. Stricter laws according to Romanosky are related to a higher amount of notifications, but it is ambiguous which aspect makes these laws strict, because American attorneys specified this classification.

8.1.1 Synthesis

The empirical research has shown that there are various incentives for compliance and that there is a first order effect of notifications. What is the relevance of this analysis for the proportionality test of Article 31 PDPR and Article 14 PCD? The first order effect is not the aim of the legislation, but a prerequisite for a second order effect. The analysis of the first order effect provides the following information.

1. There is an relative high increase in notifications after the adoption of a law
2. There is an absolute low number of notifications.
3. Representative data is important for measuring the first order effect
4. Literature review shows that enforced sanctions are balanced against reputation damage but the logic of appropriateness also plays a role.
5. In America, the height of a sanction does not play a role.

The aim of the analysis of the first order effect was to create insights in the consideration to comply with SBNLs. If the incentives for compliance are known, legislation can be designed to optimize compliance. There are many incentives and their relative importance varies. However, the problem remains that the current outcomes of the quantitative analysis cannot falsify the existence of suggested incentives. It is unknown whether the security breaches that have been notified are notified because of a cost benefit analysis or because of the logic of appropriateness. Although it is reasonable to expect that there are many situations where the cost of a notification will be higher than the cost of non-compliance, this is only a rough estimation that does not apply to all situations. For instance, the financial impact of reputation damage can vary significantly.

To illustrate this, the following scenarios are all explanations for the first order behavior that results in notifications.

Scenario 1:
Companies that comply follow the logic of appropriateness. The rest of the companies do not comply because the cost of compliance is higher than the cost of non-compliance.

Scenario 2:
Companies do not comply according to the logic of appropriateness. Some companies do comply because the cost of compliance is lower than the cost of non-compliance. Other companies do not comply because of a negative cost benefit analysis.

Scenario 3:
Companies are only compliant if the publication of a notification is inevitable, because customers are directly affected by a loss of availability, or because third parties intent to publish the data of customers.

Because it is still unclear what drives a company in complying with the law, it is hard to make recommendations on optimizing the design of the law to increase the amount of notifications.

8.1.2 The conceptual framework of the first order effect

There is uncertainty concerning the exact drivers of the observed behavior. However, the distinguished mechanisms can be outlined in a conceptual framework. The aim of the conceptual framework is to provide an overview of the variables that influence the first order effect of the SBNL. The conceptual framework is based on the synthesis of the effects in literature, quantitative and qualitative analysis.

The central element in the conceptual framework is the amount of notifications that are generated by a notification law. The notification authority administrates the amount of breaches, and therefore there are more breaches likely to be included in the database if a notification authority is present. The amount of notifications can be influenced by the willingness to comply and the range of the law.

The willingness to comply is influenced by incentives for compliance with the law that are discussed in section 4.2. Sanctioning, enforcement and confidential treatment are design parameters of the law that affect the willingness to comply positively. The willingness to comply is negatively influenced by reputation damage caused by a security breach notification. This is a negative feedback effect.

Increased Internet security as a result of the law can influence compliance. A company perceives benefits of information sharing and will increasingly value the law as appropriate. This is a positive feedback effect on the amount of notifications flowing from a SBNL.

The design parameters scope an addressees are expected to influence the range of the law. An increased scope of the law increases the amount of notifications that fall under the law. If the law covers more addresses, there are more companies that fall under the law.

Furthermore, the improvement of security by SBNLs, discussed in section 5.1.5 and 7.2.3, results in less security breaches and thus fewer notifications that have to be made. A notification law initially thus would result in an increase of notifications, because disclosure is forced. Enhanced Internet security will have a negative feedback effect on the amount of notifications.[328]

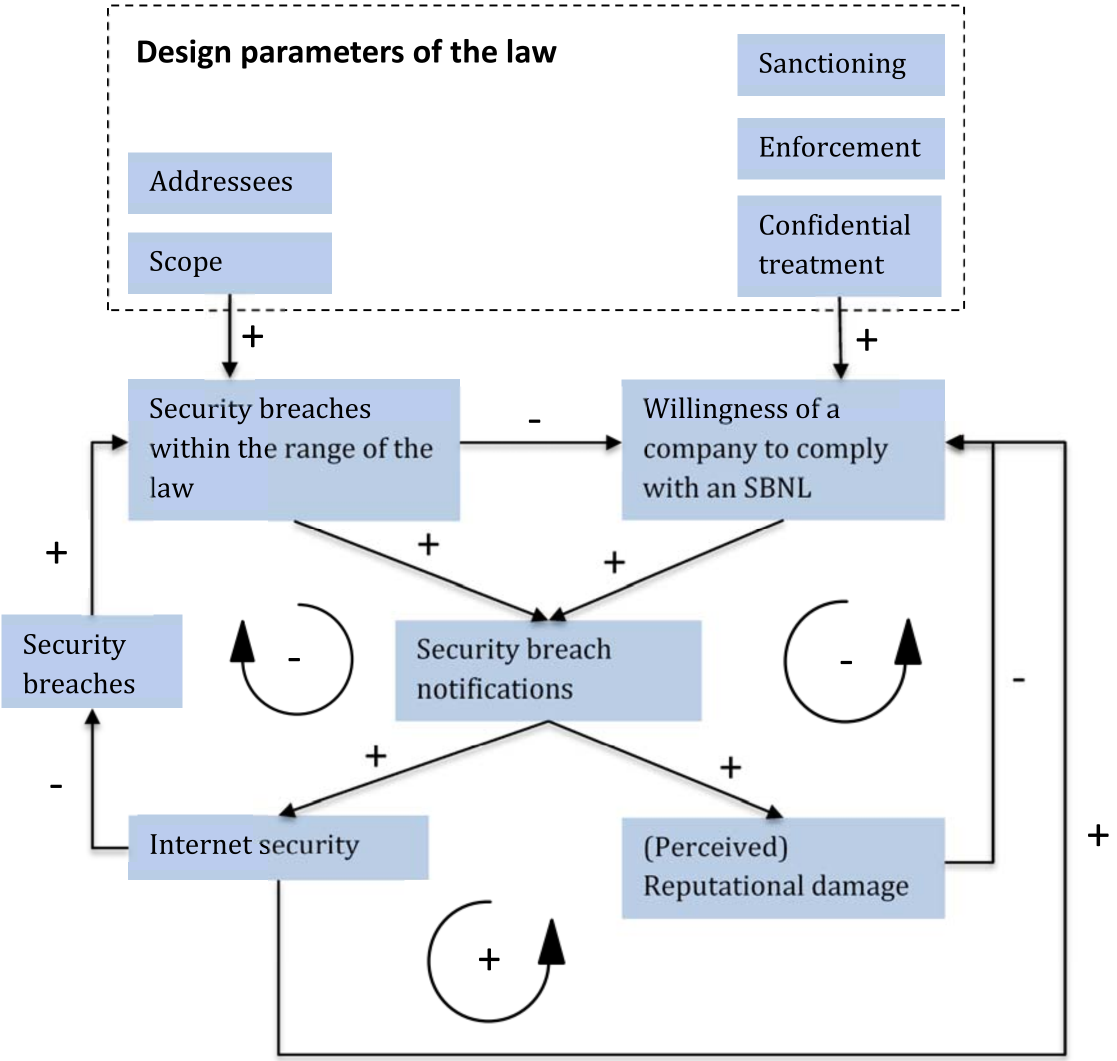

Design parameters of the law
Sanctioning
Enforcement
Addressees
Scope
Confidential treatment
+
+
Security breaches within the range of the law
-
Willingness of a company to comply with an SBNL
+
+
+
Security breaches
-
Security breach notifications
-
-
+
+
-
Internet security
(Perceived) Reputational damage
+
+

Figure 15: conceptual framework of the first order effect

[328] See section 5.1.4 of this research.

8.2 Second order effect

The second order effect of SBNLs is assessed in literature and qualitative analysis. There are positive and negative effects perceived in both literature and interviews.

The qualitative study demonstrated several positive second order effects perceived in literature and by security managers and experts, such as increased investments in security, fostered cooperation between companies (literature only), increased awareness of consumers of security breaches and faster risk mitigation. However, the positive effects can be nuanced. The security managers interviewed already shared security information with competitors, and did not see an incentive for cooperation with the government following from a security breach notification, because they did not value the government as a center of expertise. Moreover, a security expert challenged the effect of increased investments in security because the law provides an incentive to notify, not to improve security practices. Accepting the 'risk' of a notification might be less expensive than improving security practices in order to avoid notifications. This is however not confirmed in literature review or by other qualitative analysis, which implicates that the risk of not providing incentives to improve security practices at all must be perceived as low. Lastly, an increased number of security breach notifications might result in an overload of information, which could also result in disinterest and a notification fatigue instead of enhanced awareness and risk mitigation. This overload is not a big treat given the current low amount of notified security breaches. For instance, in America, about 600 million records were breached in the eight year period observed. This would entail that, on average, an American citizen would be notified twice in eight year.

8.3 Effects versus aims of the European SBNLs

The analysis conducted in part β rendered knowledge about effects of SBNLs. These effects are rendered in order to substantively answer the questions about the effectiveness of SBNLs. SBNLs are effective if they are suitable to achieve the aims pursued.

Effects	Order	Lit	Qual	Quan	Relation with legislation
Enforced sanctions	1st	V	V	X	
Reputational damage		V	V	-	
Appropriateness		V	V	-	
Benefits inf. sharing		V	V	-	
Confidential treatment		X	V	-	
Overall first order effect		-	V	V	
Faster risk mitigation	2nd (positive)	V	V	-	Aim PDPR: enhance personal data control of individuals.
Increased awareness consumers		V	V	-	Aim PDPR: trust in the digital environment
Increased security investments		V	V	-	Aim PCD: create a culture of risk management
Fostered cooperation		V	X	-	Aim PCD: enhance information exchange between the private and public sectors

Reputational costs for companies	2nd (negative)	V	V	-	
Compliance costs for companies		V	V	-	(Only) compliance costs are estimated by the Commission
Maintenance and processing costs for Member States		V	-	-	
Costs of increased investments and cooperation for companies		V	-	-	
Notification fatigue for consumers		V	-	-	-Aim PDPR: enhance personal data control of individuals. -Aim PDPR: trust in the digital environment
Incentive to notify, not to improve security for companies		-	V	-	Aim PCD: create a culture of risk management

Table 18: effects of SBNLs (V=proved or mentioned; X=disproved; "-" = not researched)

The positive effects match the aim of the PCD to 1.) create a culture of risk management and 2.) enhance information exchange between the private and public sectors respectively. The last two positive effects correspond with the aim of the PDPR to enhance personal data control of individuals.

The second order effects in literature and qualitative analysis, although they are perceptions that can be nuanced, do match the objectives pursued in legislation. But, the objectives are vaguely defined. Their attainment can be effectiveness in the legal sense, although Advocate General Sharpston stated in *Volker Schecke* that these aims need to be specific.[329] Nevertheless, the question remains what makes an SBNL effective and when an SBNL is effective.

[329] *Volker Schecke* (n 1) Opinion of AG Eleanor V.E. Sharpston, para 105.

9 Conclusions & recommendations

9.1 Conclusions on EU SBNLs

This thesis has the objective to make a contribution to the development of a European cybersecurity policy by means of the following research question:

> **To what extent does the current European Union approach concerning general SBNLs stand the proportionality test?**

The PDPR introduces a personal data SBNL. Simultaneously, the PCD requires Member States to adopt a loss of integrity SBNL. The European proposals will be discussed in this conclusion. The limitedly analyzed but closely linked subsidiarity question is discussed first. Hereafter, conclusions about the two elements of the proportionality test are formulated. Hereafter, concluding remarks about the limitations and complexity of the adhered approach are formed.

9.1.1 Subsidiarity – Necessity of a European Union approach

The necessity of the European cybersecurity approach is not fully 'scrutinized' in this thesis because subsidiarity is to great extent a political question. Therefore, the arguments for necessity have been described. From an apolitical point of view, this thesis did not find a convincing argument about the inappropriateness of a *European* approach regarding cybersecurity and SBNLs.

The Commission argues that the European Union has a leadership role in enhancing cybersecurity. The European Union argues that a *European* cybersecurity approach is necessary because of the cross border aspect of the Internet, the necessity of a uniform secure Internet for the Single Market and the protection of fundamental rights. The acceptance of a European approach is confirmed by the fact that there are a number of Cybersecurity laws, such as the FDIS and the E-privacy Directive and many policy documents that stress the importance of a European cybersecurity approach.[330]

The Commission justified the need for the proposed *European* SBNLs also by stressing the need for harmonization because of the cross border aspect of the Internet in the Single Market. The necessity of removing distortions in the Single market through a European Union SBNL approach in the PDPR is supported by the debate about SBNLs in the United States. The United States plans to unify state level SBNLs because the obligation to comply with multiple SBNLs simultaneously caused significant administrative burdens for companies.

[330] See section 2.1.2 of this research for an extensive soft law discussion.

9.1.2 Proportionality (1) – First order effect

If the European Union has an advantage in the regulation of cybersecurity, its legislation still needs to be effective. Legislation must be suitable to achieve the aim. This section discusses whether reviewed legislation is suitable to achieve the first order effect of SBNLs: breach notifications.

The SBNL in the PDPR contains severe sanctions for non-compliance. This will incentivize companies to comply with the law, although this is not supported by quantitative analysis. There are additional costs relating to enforcement of the law. In addition to this, the administrative burden for companies will be high, because they have to note all types of personal data loss. Some minor types of personal data loss, for example because an employee without rights accessed the data with minor external consequences, also need to be notified.

The Dutch initiative, this thesis' example of a loss of integrity SBNL in Article 31 PCD, lacks sanctioning as an incentive for compliance. Moreover, the benefits of information sharing are perceived to be low and confidential treatment is perceived a large incentive for compliance because of Dutch transparency laws.[331]

Relevant design parameters of the European and Dutch initiative are not clear yet. It is unknown how many resources will be assigned to the enforcement of SBNLs. It is also unknown which aspects of a security breach have to be notified and in what form the information has to be collected.

9.1.3 Proportionality (1) – Second order effect

The literature review and the qualitative study demonstrate several positive second order effects, such as increased investments in security, fostered cooperation between companies (literature only), increased awareness of consumers of security breaches and faster risk mitigation. The second order effects in literature and qualitative analysis, although they are perceptions that can be nuanced, do match the objectives pursued in legislation. But, the objectives are vaguely defined and their attainment can be effectiveness in the legal sense, but the question remains what makes an SBNL effective and when an SBNL is effective.

9.1.4 Proportionality (2) – Necessity of coexistence

European legislation must be designed in such a way, that there cannot be a less onerous way to do it. The SBNL infringes the fundamental right of freedom to conduct business because it imposes administrative burdens and reputation damage on companies, in a similar way as *Scarlet Extended*.[332] This means that if there are alternative options that impose fewer restrictions on companies, all other interests being equally protected, the current approach is not necessary, and thus not proportional (see Article 52 of the Charter).

[331] See the Dutch 'Wet Openbaarheid Bestuur' (Public administration disclosure law).

[332] *Scarlet Extended* (n 12).

From this ‘least restrictive measure’ perspective, the necessity of the (potential) coexistence of the two proposals is equivocal. The coexistence of the two initiatives is not the least restrictive way to constitute a security breach notification obligation, because it possibly imposes unnecessary administrative burdens on companies.

The PDPR and the PCD are not mutually exclusive: loss of integrity and data protection overlap. This will create some undesirable effects. First, companies have to comply with two proposals that emit different signals and incentives, which can create legal uncertainty. The confidential treatment in the PCD will not function properly if companies are simultaneously forced to publicly disclose the same information in the PDPR. Second, the legislation will be executed on a different administrative level. This will create unnecessary costs for Member States because multiple supervisory authorities need to be constituted to notify a security breach. In addition to that, it will impose unnecessary administrative burdens for companies because they have to comply with multiple regimes.

9.1.5 Limitations on measuring effectiveness

The fuzziness of the aims and the complexity of measuring effects hamper the determination of a reasonable expectation of causality between the measure and the aims pursued. The Commission sets aims that are fuzzy and hard to measure, and does not specify how these goals will be achieved through the adoptions of SBNLs. Likewise, the empirical measurement of effects in part β showed that it is complex to pinpoint effects of SBNLs. Moreover, the Commission undervalued the societal costs and adverse effects.

In my view, in the current situation, a reasonable expectation of effectiveness is not demonstrated sufficiently. In the theoretically desired situation, the goals are clear and measurable. The law is effective because the measurable aims are achieved by the measure. But, still, effectiveness is not simply attaining aims. Even if the causal relation between the measure and its aims can be proved in a narrow sense, the question remains whether the achievement of these aims is effective.

From a security economics perspective, it can be argued that the law is effective if the revenues of positive effects are higher than the societal costs of negative effects.[333] This requires an accurate empirical measurement of these effects, initiated in part β, and a quantification of these effects. Unfortunately, this approach towards effectiveness does not cover non-economic, non-measurable aims such as the protection of fundamental rights. The protection of fundamental rights is not always ‘efficient’ and can certainly not always be quantified, but European legislation must remain within the boundaries of

[333] See table 1, effects of SBNLs. One could also argue that only a *pareto improvement* of a positive effect would be preferable.

fundamental rights.[334] Moreover, the complexity of the legal interferences in the field of cybersecurity makes it impossible to provide an exhaustive balance sheet of all (expected) effects. A security economics perspective would not be the perfect means to define effectiveness, because some aims are not measurable and expected effects are complex.

Neither a legal nor an economic approach provides an optimal outcome for the definition of 'effectiveness'. There is no uniformity of what makes a law effective. Thus, still the effectiveness question remains. What is needed to determine the effectiveness of SBNLs? Who may decide when a law is effective? In a democracy, we all should decide. More concrete: the European Commission, Parliament and Council state *ex ante* in the ordinary legislative procedure the aims of the law. The European Court of Justice decides *ex post* whether the law is effective. Thus, effectiveness in redefined, as legal and economic approaches towards effectiveness are troublesome. This definition must be regarded as a starting point for further research on interpreting effectiveness of the law.

Effectiveness is the causality between a legislation and its aims defined by a democratic decision making process where as much information as possible about (potential) positive and negative effects is provided.

Thus, taking this definition into account, improving information about potential positive and negative effects is the key tool to enhance effectiveness of the law and correctly assess its necessity. The executed empirical analysis in this thesis has provided knowledge about the effects of SBNLs that can be used by the Commission. Increased availability of information about societal impact (expectations) enhances decision making of the legislature *ex ante* and the scrutiny of the Court *ex post* that determine the proportionality of cybersecurity laws. The Commission, which has the power of initiative, should invest to provide this information.

To conclude, additional information about effects of legislation on society will improve the quality of draft legislation and the judicial decision about proportionality. For example, information about the adverse reputation damage on companies, demonstrated in this thesis, will play a vital role when judging about the infringement on the freedom to conduct business. Additional information about effects will not be decisive in a judicial decision, since also non measurable effects need to be balanced and (expected) effects have a certain margin of error. The proportionality test as such must be seen in relation to these inherent flaws within measuring effectiveness of the law on society. Often, causality between the measure and the aim can and will not be 'proven' scientifically by the legislature and the Court. Nevertheless, the proportionality principle has been a corner stone of European Law to analyze the effectiveness and necessity of legislation. Further enhancement of the execution of this principle by improving

[334] In countries such as China, where there is more limited attention for fundamental rights, governmental policies, for instance the construction of a highway, can be executed far more efficiently than in the European Union.

information about societal effects increases the democratic legitimacy of European Union law.

9.1.6 Complexity of measuring effects

The quantitative analysis on the effects of design parameters of SBNLs proved to be complex, because of the following reasons.[335]

- The dataset does not cover all breaches that were notified in the observed period.
- The number of companies that does not comply with the law cannot be estimated.
- Breaches in the database do not have a similar impact. The size of the impact is hard to estimate, amongst others because breaches with a smaller number of records generally have a large impact per record.
- The comparison of the situation before the adoption of a law with the situation after the adoption of a law is difficult. The dataset did not clarify whether a breach in the database flowed from an obligation under an SBNL, which makes it impossible to identify additional notifications through the SBNL.
- The embedment of several feedback effects, such as Internet security and reputation damage, increased the complexity of the model.

This research experience is highly relevant for an *ex post* effectiveness test of the SBNL by the European Commission. When monitoring the law this complexity should be taken into account. A central documentation of breach notifications in the European Union would be first step to enhance the availability and representatives of breach data. Such a dataset requires detailed thought about amongst others assumptions regarding the degree of non-compliance, the size of the breach and feedback loops. Without such assumptions, the validity of the results in the database, and consequently the effectiveness test, would be hampered.

9.2 Recommendations

This thesis provides three types of recommendations. There is still ambiguity about the effectiveness of the law. Nevertheless, recommendations regarding enhancement of the PCD and the PDPR are made. These recommendations will enhance the positive effects of the laws, but the implementation of these recommendations will not immediately lead to a decisive answer about causality between the measure and its aims. To enhance effectiveness further, information about effects needs to be improved. Before the adoption of the law, a reasonable expectation of effectiveness should be given. After the adoption of the law, (tools to perform) an effectiveness test needs to be provided.

[335] For a more extensive description of assumptions regarding the dataset, see chapter 5 of this research.

9.2.1 Regarding the enhancement of the legislative initiatives

Enhance the PCD and the Dutch initiative.
The PCD and the Dutch initiative need adjustment. An adjustment of the proposals can increase compliance with the law, improve positive second order effects and mitigate negative effects. This concerns clarity of the scope, the added value of the supervisory authority and the reduction of the administrative burden for companies. The ambiguity about the scope will be improved by a clear definition of what is meant by a 'significant loss of integrity' in the PCD and 'societal shock' in the Dutch initiative. Furthermore, the supervisory authority, such as the NCSC, must have added value in mitigating the breach. Added value implicates technical cybersecurity knowledge to assist in mitigating security breaches. Otherwise, companies will not have incentives to comply with the law. Finally, a notification that contains simultaneously a loss of integrity and personal data breach needs to be forwarded automatically to the European supervisory authority for the PDPR. This will reduce administrative burdens for companies because this excludes the need to make a separate notification for the PDPR.

Adopt a single European SBNL for both personal data and loss of integrity.
The proposed mixed approach will create legal uncertainty and unnecessary administrative burdens because companies would have to comply with overlapping legislation with multiple requirements and administrative bodies. A less restrictive equally effective policy option is recommended to the European Commission. It is recommended to extend Article 31 PDPR with a loss of integrity requirement and to abolish Article 14 PCD. This results in one single SBNL focusing on both personal data and a significant loss of integrity. It still remains necessary to provide a clear definition of the threshold of a breach and provide the supervisory authority with technical cybersecurity knowledge.

9.2.2 A reasonable expectation of effectiveness before the adoption of the law

This thesis recommends to improve the measurement of (the expectation of) effectiveness before and after the adoption of the law. These recommendations can be used for improving European law in general and the PDPR and PCD in particular. As already mentioned, effectiveness is redefined as follows to give a starting point for further research:

> Effectiveness is the causality between a legislation and its aims defined by a democratic decision making process where as much information as possible about (potential) positive and negative effects is provided.

Hence, it is the duty of the European legislature to provide as much useful information as possible about the effects of the laws to enable scientific analysis of the law and improve the democratic legitimacy.

Operationalize aims that are measurable
This thesis argues that the current aims of the PDPR and the PCD are ambiguous concepts that need to be operationalized. Operationalization is the process of redefining an ambiguous concept to make it measurable in order to perform empirical

observations. The Commission has the primary task to redefine the aims of the legislation. Nevertheless, this thesis research proposes some starting points for this process.

The main aims of the PDPR are to enhance personal data control and trust in the digital environment in order to protect to fundamental right of data protection. This thesis recommends two alternative approaches to operationalize these aims.[336] The first approach regards the aims as *perceptions* of European citizens. Hence, the aim would be to improve the perception of personal data control and trust in the digital environment, by European citizens. The second approach uses proxies to operationalize aims. A proxy is a measurable unit that can be used to represent a non-measurable unit, to approximate or substitute the current aims. The degree of online activity of consumers, for instance the percentage of people that use the Internet, is a general proxy for personal data control and trust in the digital environment. More specific proxies concern activities on the Internet that are vulnerable for personal data theft, such as online banking, shopping or online localization. The first order effect of the legislation, the number of security breaches notified, can also be a proxy for effectiveness of the law. Regarding this proxy, one would first expect an increase and *ceteris paribus* a decrease of the number of security breaches caused by increased security.[337]

The main aim of the PCD is to create a culture of risk management. A culture of risk management also needs further operationalization, for instance by defining it as the perception of companies on the level of risk management in their sector. A proxy for the culture of risk management is the amount and quality of the cybersecurity information exchange between private parties and the supervising authority. Preferably, these measurable units should replace the current fuzzy aims to reduce ambiguity, provided that no valuable information is lost in the process of operationalization.

Explicitly mention aims that are not measurable such as fundamental rights

It should also be stated explicitly when aims are not measurable. The PDPR and the PCD both aim to safeguard fundamental rights.[338] Fundamental rights that are associated with the aims of the legislation, such as the freedom of speech and the freedom of expression, have an intrinsic value which cannot be operationalized. These important non measurable aims should be included *separately* as informative input for a democratic legislative decision making process that decides about the legislation (and its aims).

Operationalize measurable side effects

An effective consideration of the democratic decision making process necessitates an extensive overview of potential negative effects of the SBNL as well.[339] Currently, the cost estimation of the Commission is undervalued compared with the total societal costs

[336] There are more approaches imaginable; this is a suggestion for further research.
[337] Although this also has some complex side-effects, see for instance section 8.1 of this research.
[338] See section 2.3.2 of this research.
[339] For instance, because the PDPR and PCD potentially infringe the fundamental right to conduct business, see section 3.2.4 of this research.

of an SBNL. The European Commission should include the negative reputational effects of companies into its impact assessment as well as expected administrative and processing costs.

Provide a reasonable expectation of causality between the law and the aims pursued
An extensive overview of measurable and non-measurable positive and negative effects of the proposed law will be available when the Commission follows up to the aforementioned recommendations. It is not possible to *measure* these effects before the adoption of the law, but it is possible to give a reasonable expectation of causality and the aims pursued. However, currently, the Commission did not substantiate in what way the SBNL is suitable to achieve the aims pursued. Therefore, it is recommended to thoroughly study the expected effects of legislation in academic literature, by means of secondary available comparative (quantitative) analysis and by expert interviews.[340] This threefold approach, adhered in this thesis, has enhanced the knowledge about expected effects and needs further development and a wider application.[341] A conceptual diagram can clarify the effects to enhance the information of the decision maker.[342]

Deduct the discussion about the desirability of the legislation to normative choices.
The combination of tightly operationalized measurable aims and explicitly stated non measurable aims allows for a more enhanced discussion about the desired effects of the legislation. Ideally, the expected effects of the measurable part of the legislation will be quantified in order to clarify and structure the discussion about the desirability of the law. Consequently, the discussion solely concerns normative choices about the balance between non quantifiable effects with the sum of the measurable positive effects and negative effects.

9.2.3 Tools to measure effectiveness after the adoption of the law

Register perceptions of the law and relevant proxies
The perception of companies and consumers regarding the law and relevant proxies need to be registered. The operationalized aims of the legislation that concern perceptions such as the perception of trust in the digital environment must be measured by the Commission after the introduction of the law.[343] Simultaneously, the Commission must measure the perception of companies and consumers of effectiveness of the law as such, to assess whether the parties involved with the law regard the law as effective. Such questionnaires can aid to give a more qualitative indication on the effectiveness of

[340] Such as performed in this thesis in part ß.
[341] Currently the fuzziness of the aims and the complexity of measuring effects hamper the determination of a reasonable expectation of causality between the measure and the aims pursued.
[342] See section 8.1.2 of this research for a conceptual diagram of the first order effect of SBNLs.
[343] Of course, there is much more complexity involved with attributing the possible effects operationalized in such a questionnaire or dataset to the existence of the law, see chapter 6 of this research.

the law.[344] Apart from perceptions measured in surveys, proxies are another way to measure effectiveness of the law and need to be registered as well.

Register data about security breaches

It is important to measure effects after the introduction of the law to scrutinize the claims about expected effects made before the introduction of the law. The information about security breaches that are notified under the obligation flowing from the SBNL needs to be registered centrally. The central registration of these breaches would provide a representative longitudinal dataset. This dataset can be used to measure to which extent the SBNL is capable of incentivizing companies to notify security breaches.[345] The details of the security breach can provide information about the attainment of the second order effects of the legislation. Consequently, the information should be included in a security breach notification to gain more insights in the second order effects.[346] Apart from information about the security breach, also the costs of processing, monitoring and enforcement should be registered.[347] The information that should be included is displayed below:

- General information:
    - A detailed description about the circumstances of a security breach.
    - The industry of the company that notified.
    - An approximation of the damage of the breach:
        - Reputation damage for the company.
        - Losses for consumers
        - Damage for society because of (for instance) unavailable services
- Information regarding a personal data breach:
    - The amount of records of personal data theft.
    - The type of personal data theft.
- Information regarding a loss of integrity breach:
    - The level of defense of security systems that is breached
    - Whether there is actual physical damage to computer systems or solely potential damage

9.3 Directions for further research

The legal position and societal effects of security breach notification laws deserves further empirical study. Another promising line of research would be to identify the costs of the SBNL notification system. Research showed that indirect costs are mostly

[344] See for instance the Eurobarometer.

[345] This dataset can do this better than the dataset used in chapter 5, because it contains exclusively and exhaustively security breaches from the SBNL.

[346] This is not an exhaustive list, but mainly a synthesis of suggestion from interviews, see section 7.2.4 of this research.

[347] Often, the indirect defense costs of Internet security are more expensive than the losses itself, see section 1.1.3 of this research.

higher than direct costs. Further experimental observations are needed to estimate the impact of stricter laws on compliance. A challenging task for further research would be to unravel the effect of Internet insecurity on the amount of security breach notifications. The design and complexity of enforcement of an SBNL also deserves further attention. Moreover, some thought is needed on the approach to operationalize fuzzy goals.

A higher-level line of research concerns definition of effectiveness, provided in the concluding pieces of this thesis. Within this definition, effectiveness is largely defined as the outcome of a democratic decision making process. This has the consequence that effectiveness is transformed from an objective criterion towards an intersubjective concept of truth, largely depending on the functioning of democracy. This deserves a further legal, political and philosophical exploration.

Bibliography

General bibliography

Literature

Ayres I and Braithwaite J, *Responsive Regulation: Transcending the Deregulation Debate* (Oxford University Press, 1992).

Asghari H, 'Botnet Mitigation and the Role of ISPs' (Master Thesis, Delft, University of Technology).

van den Brink A, 'The Substance of Subsidiarity: The Interpretation and Meaning of the Principle after Lisbon' in Martin Trybus and Luca Rubini (eds) *The Treaty of Lisbon and the Future of European Law and Policy* (Edward Elgar Publishing 2012).

Chalmers D, Davies G and Monti G, *European Union Law* (second edition, Cambridge University Press 2010).

Graig P and de Búrca G, *EU Law - Text Cases and Materials* (fifth edition, Oxford University Press 2011).

Heck R, *Multilevel and Longitudinal Modeling with IBM SPSS* (Routledge, 2010).

Hill J.F, 'Internet Fragmentation: Highlighting the Major Technical, Governance and Diplomatic Challenges for U.S. Policy Makers' (Paper, Harvard Kennedy School 2012).

Jans J, de Lange R, Prechal S and Widdershoven R, *Europeanisation of Public Law* (Europa Law Publishing 2007).

de Jong M, Lalenis K and Mamadouh V, *The Theory and Practice of Institutional Transplantation* (Kluwer, 2002).

Klip A, *European Criminal Law, an integrative approach* (second edition, Intersentia 2012).

de Leeuw K & Bergstra J. (eds.), *The History of Information Security: A Comprehensive Handbook* (Elsevier, 2007).

Lenz C and Borchardt K, *EU-Verträge Kommentar nach dem Vertrag von Lissabon* (Bundesanzeiger Verlag 2010).

Meijer E, ‘Convention on cybercrime, Data protection in information systems through criminal law; a comparison between the EU and the US.’ (Master Thesis, Utrecht University, 2012).

Renda A, *Impact Assessment in the EU, The State of the Art and the Art of the State* (CEPS Paperbacks 2006).

Senden L and Prechal S, ‘Differentiation in and through Community Soft Law’, in De Witte B, Hanf D and Vos E (eds),*The Many Faces of Differentiation in EU Law* (Intersentia, 2001).

Seltman H, *Experimental Design and Analysis* (Published online, 2009).

Twisk JWR, *Applied Multilevel Analysis* (Cambridge University Press, 2006).

Tyler Moore and Ross Anderson, ‘Internet Security’ in M. Peitz & J. Waldfogel (Eds.), ‘The Oxford Handbook of the Digital Economy’ (Oxford University Press 2011).

Verbeek M, *A Guide to Modern Econometrics* (Fourth Edition, Wiley, 2012).

Verschuren P & Doorewaard H, ‘*Designing a research project*’ (Second edition, Eleven International Publishing 2010).

de Vries SA, ‘The Protection of Fundamental Rights within Europe’s Internal Market after Lisbon – An Endeavour for More Harmony’ in S. A. de Vries, Ulf Bernitz and Stephen Weatherill *The Protection of Fundamental Right in the EU after Lisbon* (Hart Publishing, 2013).

Watson A, *Legal Transplants, An Approach to Comparative Law* (Second Edition, University of Georgia Press, 1994).

Zealke D, *Making Law Work, Environmental Compliance & Sustainable Development* (International Law Publishers 2005).

Journal Articles

Bobek M, ‘Joined Cases C-92/09 and C-93/09, Volker und Markus Schecke GbR and Hartmut Eifert, Judgement of the Court of Justice (Grand Chamber) of 9 November 2010 N.Y.R. (Annotation)’ (2011) 48(6) *Common Market Law Review* 2005.

Burdon M, Lane B, von Nessen P, ‘Data Breach Notification Law in the EU and Australia, Where to now?’ (2012) 28(3) *Computer Law and Security Review* 296.

Calderoni F, ‘The legal framework for cybercrime: striving for an effective implementation’ (2010) 54(5) *Crime, Law and Social Change* 339.

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

De Hert P and Papakonstantiou V, 'The proposed Data Protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals' (2012) 28(3) *Computer Law and Security Review* 130.

Dimitrakopoulos DG, 'The transposition of EU law: Post-decisional politics and institutional autonomy' (2001) 7(4) *European Law Journal* 442-458.

Etienne J, 'Compliance Theory: A Goal Framing Approach' (2011) 33(3) *Law & Policy* 305.

Goel S, and Shawsky H, 'Estimating the market impact of security breach announcements on firm values' (2009) 46 Information and Management 404.

Gordan M, 'When should companies go public following a security breach?' (2006) 9 *Computer Fraud and Security* 17.

Jans JH, 'Proportionality Revisited' (2000) 27(3) *Legal Issues of Economic Integration* 239.

Hunton P, 'The growing phenomenon of crime and the Internet: A cybercrime execution and analysis model' (2009) 25 *Computer Law & Security Review* 528.

Ko M and Dorantes C, 'The impact of information security breaches on financial performance of the breached firms: an empirical investigation' (2006) 16(2) *Journal of Information Technology Management* 13.

Moore T, 'The economics of cybersecurity: Principles and policy options' (2010) 3(3-4) *International Journal of Critical Infrastructure Protection* 103.

Munterman J and Roßnagel H, 'On the Effectiveness of Privacy Breach Disclosure Legislation in Europe: Empirical Evidence from the US Stock Market' (2009) 5838 *Lecture Notes in Computer Science* 1.

Romanosky S, Telang R, Acquisiti A, 'Do Data Breach Disclosure Laws Reduce Identity Theft?' (2011) 30(2) *Journal of Policy Analysis and Management* 256.

Schwartz PM and Janger EJ, 'Notification of Data Security Breaches' (2007) 105 *Michigan Law Review* 913.

Sutinen J. and Kuperan K, 'A socio-economic theory of regulatory compliance' (1999) 26 (1/2/3) *International Journal of Social Economics* 174.

Tyler TR, 'Compliance with Intellectual Property Laws: A Psychological Perspective' (1999) 29 *New York University Journal of International Law and Politics* 219.

Veltsos JR, 'An Analysis of Data Breach Notifications as Negative News' , (2012) 75(2) *Business Communication Quarterly* 192.

Online articles and papers

Anderson R, 'Why Information Security is Hard – An Economic Perspective (*University of Cambridge*, December 2001) <http://www.cl.cam.ac.uk/~rja14/Papers/econ.pdf> accessed 25 June 2013.

Anderson R, Barton C, Bohme R, Clayton R, van Eeten MJG, Levi M, Moore T and Savage S, 'Measuring the Cost of Cybercrime' (2012) Workshop on Economics of Information Security 6/2012 <http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf> accessed 7 January 2013.

Anderson R, Böhme R, Clayton R and Moore T, 'Security Economics and the Internal Market' (*ENISA*, 31 January 2008) <http://www.enisa.europa.eu/publications/archive/economics-sec>, Accessed 10 December 2012.

Arnbak A and van Eijk N, 'Certificate Authority Collapse, Regulating Systemic Vulnerabilities in the HTTPS Value Chain' (2012) TRPC, 20 <http://papers .ssrn.com/sol3/papers.cfm?abstract_id=2031409 > accessed 8 January 2012.

Deirdre Mulligan, 'Security Breach Notification Laws: Views from Chief Security Officers' (*Unversity of Berkeley School of Law*, December 2007) <http://www.law.berkeley.edu/files/cso_study.pdf> accessed 11 June 2013.

Drewer D & Ellermann J, 'Europol's data protection framework as an asset in the fight against cybercrime' (*Europol*, 19 November 2012) <https://www.europol.europa.eu/sites/default/files/publications/drewer_ellermann_article_0.pdf> accessed 11 June 2013.

'Fraude report Internet banking and skimming' (*Nederlandse Vereniging van Banken*, 2012). <http://www.veiligbankieren.nl/nl/nieuws/fraude-Internetbankieren-stijgt-eerste-half-jaar-met-14_.html> accessed 11 June 2013.

Hudson P, 'Safety Culture, Theory and Practice' (*Centre for Safety Science, Leiden University.* 1999), 3 <http://ftp.rta.nato.int/public//PubFulltext/RTO/MP/RTO-MP-032///MP-032-08.pdf> accessed 13 June 2013.

Kincaid C, 'Guidelines for Selecting the Covariance Structure in Mixed Model Analysis' (*SUGI*, 10 April 2005) 30 <http://www2.sas.com/proceedings/sugi30/198-30.pdf> accessed 13 June 2013.

Pélissié du Rausas M, 'Internet Matters: The Net's sweeping impact on growth, jobs and prosperity'. (*McKinsey Global Institute*, May 2011). <http://www.mckinsey.com/insights/high_tech_telecoms_Internet/Internet_matters> accessed 27 December 2012.

Steunenberg B and Voermans W, 'The transposition of EC Directives: A comparative study of instruments, techniques and processes in six Member States' (*WODC*, 2006) <https://openaccess.leidenuniv.nl/bitstream/handle/1887/4933/5_360_361.pdf?sequence=1> accessed 11 June 2013.

Van Eeten MJG, Bauer JM, Asghari H, Tabatabaie S, 'The Role of Internet Service Providers in Botnet Mitigation: an Empirical Analysis based on Spam Data' (2010) OECD STI Working Paper 2010/5 <http://search.oecd.org/officialdocuments/displaydocument_pdf/?cote=DSTI/DOC%282010%295&docLanguage=En> accessed 11 June 2013.

Van Eeten MJG and Bauer JM, 'Security Decisions, Incentives and Externalities' (2008) (OECD STI Working Paper 2008/1) <www.oecd.org/Internet/ieconomy/40722462.pdf> accessed 14 June 2013.

European Union policy documents

European Commission, 'A strategy for a Secure Information Society – Dialogue, partnership and empowerment' (Communication) COM (2006) 251 final.

European Commission 'Communication on Network and Information Security' (Communication) COM (2001) 298 final.

European Commission, 'Cybersecurity Strategy for the European Union' (Joint Communication) JOIN (2013) 1 final.

European Commission 'Impact Assessment accompanying the Proposal for a Directive of the European Parliament and of the Council Concerning measures to ensure a high level of network and information security across the Union' (Impact assessment of the Cybersecurity Directive) SWD (2013) 32 final.

European Commission 'Impact Assessment accompanying (proposed) Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data' (Impact Assessment of the Data Protection Regulation) SEC(2012) 72 final.

European Commission, 'Legal Analysis of a Single Market for the Information Society' (*DLA Piper*, 2009) <http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=7022> accessed 10 June 2013.

European Commission, 'Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience' (Communication) COM (2009) 149 final.

European Commission, 'Report from the Commission to the Council Based on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems (Communication) COM (2008) 448 final.

European Commission, 'Regulatory framework for electronic communications in the European Union Situation in December 2009' (*European Commission*, 2009) <http://ec.europa.eu/information_society/policy/ecomm/doc/library/regframeforec_dec2009.pdf> accessed 10 June 2013.

European Council, 'The Stockholm Programme – An open and secure Europe serving and protecting citizens' (Notice) [2010] OJ C 115/01.

European Commission, 'Towards a general policy on the fight against cybercrime' (Communication) COM (2007) 267 final.

Dutch policy documents

'Meldplicht Security Breaches' *Kamerstukken II* 2012/7, 26643, nr.247, 1 (letter to the Dutch Lowerhouse).

Ivo W. Opstelten 'Brief Meldplicht en interventiemogelijkheden (Ministry of Safety and Justice, 6 July 2012) <http://www.nctv.nl/Images/brief-cyber-meldplicht-en-interventie_tcm126-443885.pdf> accessed 11 June 2013.

Documents from websites

'2011 Cost of Cyber Crime Study' (*Ponemon Institute*, August 2011). <http://www.hpenterprisesecurity.com/collateral/report/2011_Cost_of_Cyber_Crime_Study_August.pdf> accessed 30 November 2012.

'Banken beloven informatie over cyberaanvallen onderling te gaan delen' (*Tweakers*, 15 April 2013) <http://tweakers.net/nieuws/88507/banken-beloven-informatie-over-cyberaanvallen-onderling-te-gaan-delen.html> accessed 13 June 2013.

Barlow JP, 'Declaration of Internet independence' (*eff*.org, 9 Februari 1996) <http://w2.eff.org/Censorship/Internet_censorship_bills/barlow_0296.declaration> accessed 9 January 2013.

'Cybersecurity Assessment Netherlands'. (*National Cyber Security Centre*, 19 September 2012). <https://www.ncsc.nl/english/current-topics/ news/ncsc-publishes-cyber-security-report-2012.html> accessed 21 April 2013.

'Cyber Security Report 2012' (*National Cyber Security Centre,* 19 September 2012), 22-34 < https://www.ncsc.nl/english/current-topics/news/ncsc-publishes-cyber-security-report-2012.html> accessed 11 June 2013.

'Data Breach Notification Laws by State' (*CLLA*, December 2012) <http://www.clla.org/documents/breach.xls> accessed 12 June 2013.

‘Data, Data everywhere’ (*The Economist,* 25 February 2010) <www.economist.com/node/15557443> accessed 11 June 2013.

‘Digital Agenda for Europe’ (*European Commission*, 2013) <http://ec.europa.eu/digital-agenda/> accessed 21 January 2013.

‘Eurobarometer 390 for the Netherlands’ (*European Commission*, 2012) <http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_fact_nl_en.pdf> accessed 7 January 2012.

‘Eurobarometer 390’ (*European Commission*, 2012), 61 <http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf> accessed 7 January 2012.

‘Firms in U.S. states’ (*Census.gov*, 2013) <http://www.census.gov/econ/susb/> accessed 13 June 2013.

‘Het Diginotarincident , Waarom digitale veiligheid de bestuurstafel te weinig bereikt’ (Onderzoeksraad voor de veiligheid, 2012). <http://www.onderzoeksraad.nl/index.php/ onderzoeken/onderzoek-diginotar/> Accessed 6 January 2012.

‘Internet penetration rate’ (*PEW Internet,* 2012) <http://pewInternet.org/Reports/2012/Digital-differences/Main-Report/Internet-adoption-over-time.aspx> accessed 12 June 2013.

‘Internet statistics’. <www.Internetworldstats.com> accessed 14 April 2013.

‘Interview Mikko Hypponen’ (*Tweakers,* 20 Oktober 2012) <http://tweakers.net/video/6478/mikko-hypponen-over-cybercrime-en-digitale-oorlog.html> accessed 22 October 2012.

‘Overview Security Breaches’ (*NCSL*, 2013) <http://www.ncsl.org/issues-research/telecom/overview-security-breaches.aspx> accessed 2 February 2013.

‘Population in U.S. states’ (*Internet World Stats*, 2013) <http://www.Internetworldstats.com/unitedstates.htm> accessed 12 June 2013.

‘Proposal on a European Strategy for Internet Security’ (*European Commission Roadmap,* November 2012) <http://ec.europa.eu/governance/impact/planned_ia/docs/2012_infso_003_european_Internet_security_strategy_en.pdf> accessed 12 June 2013.

‘Press release on Symantec Security Report’ (*Symantec*, 7 September 2011) <www.symantec.com/about/news/release/article.jsp?prid=20110907_02> accessed 28 November 2012.

‘R-square statistics in SPSS Mixed Models’ (*IBM support*, 9 July 2011) <http://www-01.ibm.com/support/docview.wss?uid=swg21481012> accessed 13 June 2013.

Security Breach Notification Chart (*Perkins*, 2013) <http://www.perkinscoie.com/files/upload/LIT_09_07_SecurityBreachExhibits2.pdf> accessed 4 July 2013.

'State Data Security Breach Notification Laws' (*Mintz Levin*, 1 December 2012) <http://www.mintz.com/newsletter/2007/PrivSec-DataBreachLaws-02-07/state_data_breach_matrix.pdf> accessed 13 June 2013.

'State Data Breach Stature Form' (Baker Hostetler, 2013) <http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/State_Data_Breach_Statute_Form.pdf> accessed 13 June 2013.

'The Privacy Rights Clearing House DataBase' (*PrivacyRights.org*, 2013). From <https://www.privacyrights.org/data-breach> accessed 1 February 2013.

'US GDP' (*US Government Revenue*, 2013) <http://www.usgovernmentrevenue.com> accessed 13 June 2013.

'Waterinstallatie beschadigd bij cyberaanval' <www.automatiseringgids.nl/nieuws/2011/47/waterinstallatie-beschadigd-bij-cyberaanval> accessed 11 June 2013.

Treaties, Case-law and Legislation

Treaties and protocols

Charter of Fundamental Rights of the European Union [2000] OJ C364-1.

Protocol (No 2) on the Application of the Principles of Subsidiarity and Proportionality [2007] OJ C-310/207.

Consolidated Version of the Treaty on European Union [2008] OJ C115/13.

Consolidated Version of the Treaty on the Functioning of the European Union [2008] OJ C115/47.

Convention on Cybercrime 2001.

Case-law

Case C-26/62 *Van Gend en Loos* [1963] ECR 1.

Case C-6/64 *Costa/ENEL* [1964] ECR 585.

Case 29/69 *Erich Stauder v City of Ulm – Sozialamt* [1969] ECR 419.

Case 93/71 *Leoniso v. Italian Ministry of Argiculture* [1972] ECR 293.

Case 41/74 *Van Duyn* [1974] ECR 1337.

Case 80/86 *Kolpinghuis* [1987] ECR 3969.

Case C-260/89 *Ellinki Radiophonia Tileorassi AE* (*ERT*) *v Dimotiki Etairia Pliroforissis and Sotirios Kouvelas* [1991] ECR I-2925.

Case C-379/98 *Germany v Parliament and Council (Tobacco Advertising I)* [2000] ECR I-8419.

Case C-112/00 *Schmidberger* [2003] ECR I-5659.

Case C-105/03 *Criminal proceedings against Maria Pupino* [2005] ECR I-5285.

C-275/06 *Promusicae* [2006] ECR I-271.

Cases C-152/07 & C-154/07 *Arcor* [2008] ECR I-5959.

Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* [2010] ECR I-0000.

Case C-70/10 *Scarlet Extended v SABAM* [2011] ECR I-0000.

Joined Cases -411/10 and C-493/10 *N.S. v Secretary of State for the Home Department* [2011] ECR I-0000, paras 64-69.

European Union (proposed) legislation

Council Directive (EC) 95/46 EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995], OJ L 281.

Council Directive (EC) 96/96 on the approximation of the laws of the Member States relating to roadworthiness tests for motor vehicles and their trailers [1996] OJ L49.

European Commission 'Guidelines on the method of setting fines imposed pursuant to Article 23(2)(a) of Regulation No 1/2003 (Leniency Policy)' [2006] OJ L210/02.

Council Directive (EC) 2004/48 on the enforcement of intellectual property rights [2005] OJ L 195/16.

Framework Decision (FD) 2005/222/JHA on attacks against information systems [2005] OJ L 69/67.

European Commission 'Proposal for a Directive on attacks against information systems and repealing Council Framework Decision 2005/222/JHA' (Proposal for Directive) COM (2010) 517 final.

Council Regulation (EC) 1290/2005 on the financing of the common agricultural policy [2005] OJ L209/1 as amended by Council Regulation (EC) 1437/2007 [2007] OJ L322/1.

Council Directive (EC) 2009/136 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation(EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

Council Directive (EC) 2009/140 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services [2009] OJ L337/37.

European Commission 'Proposal for a Regulation concerning the European Network and Information Security' (Proposed Regulation) COM (2010) 521 final.

European Commission 'Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data' (Proposed Data Protection Regulation) COM (2012) 11 final.

European Commission 'Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union' (Proposed Cybersecurity Directive) COM (2013) 48 final.

Dutch legislation

Telecommunicatiewet <http://wetten.overheid.nl/BWBR0009950> accessed 19 June 2013.

Wet Openbaarheid Bestuur <http://wetten.overheid.nl/BWBR0005252> accessed 19 June 2013.

Experts consulted

Official interviews:

Name	Position / Institution
Mr. A. Engelfriet	Associate, IT-Recht
Mr. R. Prins	Founder, Fox IT
Mr. R. Ragetlie	Risk manager, Brabant Water
Mr. W. Vrijssen	Security manager, Vodafone

Exploratory interviews:

Name	Position / Institution
Mr. A. Arnbak	PhD candidate, University of Amsterdam
Mr. H. Asghari	PhD candidate, TU-Delft
Mr. F. Bisogni	PhD candidate, TU-Delft
Mr. T. van den Brink	Associate Professor, Utrecht University
Mr. D. van Duren	Policy advisor, Ministry of Security and Justice
Mr. B. Eidhof	PhD candidate, University of Amsterdam
Ms. B. Givens	Director, Privacy Rights Clearinghouse
Mr. J. Leenheer	Policy advisor, NCSC
Mr. R. Philipse	Business analyst, Google Inc.
Ms. N. Saanen	Associate Professor, TU-Delft
Mr. B. Rijkhoek	Policy advisor, Ministry of Security and Justice
Mr. S. Romanosky	Research fellow, Carnegie Mellon University
Mr. H. Verweij	Policy advisor, NCSC

Appendix A – Interview template

Total duration: 60 minutes

1. Explanation of subject and introduction (5-10 minutes)

- Security Breach Notification Laws (SBNL)
  - Dutch, European initiatieven & American legislation
  - Context of the interview: Increase knowledge about effects and support of the dataset.
- Goal of the interview
  - Insights of the respondents in the first and second order effects of an SBNL
  - Comments of the respondents in the procedure adhered in the dataset.
- Joint goal:
  - Rethink SBNLs and the benefits and necessity of current legislation.

Main subject

Effects of an SBNL (20 minutes)

What consideration does a company make to notify of withhold a notification?
What do you expect of the effectiveness of an SBNL? Do you expect more notifications after an SBNL?
Which variables are essential for the (first order) effectiveness of SBNLs?
What are important characteristics of a breach or a company that determine effectiveness of an SBNL? (For instance the severity of a breach, or the type of company that should be notified?)
How would you measure effectiveness of SBNLs?

5. Database specific (15 minutes)

General questions

What would be the effect of higher sanctions on compliance? (var. Sanctioningv3 ; Not AG)
What would be the effect of confidential treatment of the notification such as the NCSC practice? (also, private cause of action, not_ag)
What would be the effect of the scope of the SBNL?

-Representation of results from the statistical analysis-

Representativeness:

How do you value a database that contains breaches of 0,05% of the U.S. companies?
The current dataset displays al kinds of notifications (consumers, third parties etc.). How can we filter for these sources?
Breaches do not have equal sizes? How could we rank breaches?

In kaart brengen wet

What would be a decent approach to map different characteristics of the law?

Verbeteringen dataset

How can we further improve our data and generate more data?

How the registration of data be improved?

Other/extra:

How does a security breach notification function at companies? (5 minutes)

- What does it mean for companies to process security breaches?
    - How does the security breach procedure function?
    - Who is responsible?
    - What is the speed of a notification?

Discuss second order effects found in literature. (5-10 minutes)

6. Wrap up, conclusions (5-10 minutes)

- Extra questions/remarks
- Suggestions for next steps, relevant contacts.

Appendix B – Classifications of the American SBNLs

State	Introduction date	Sanctioning	Private_action	Strictness_Romanosky	Scope_law	Not_cust credit	Not_ag
Alabama	no SBNL	0	0	0	0	0	0
Alaska	2009	0	1	0	1	1	0
Arizona	2007	0	0	0	0	0	0
Arkansas	2005	0	0	0	1	0	0
California	2003	0	1	1	1	0	1
Colorado	2006	0	0	0	0	1	0
Connecticut	2006	0	0	0	0	0	1
Delaware	2005	0	0	0	0	0	0
Florida	2005	1	0	0	0	1	0
Georgia	2005	0	0	0	1	1	0
Hawaii	2008	0	0	1	0	1	1
Idaho	2006	0	0	0	0	0	1
Illinois	2006	0	0	0	0	0	0
Indiana	2006	1	0	0	0	1	1
Iowa	2008	0	0	0	1	0	0
Kansas	2006	0	0	0	1	1	0
Kentucky	no SBNL	0	0	0	0	0	0
Louisiana	2006	1	1	0	0	0	1
Maine	2006	1	0	0	1	1	1
Maryland	2008	0	1	1	1	1	1
Massachusetts	2007	0	1	1	1	1	1
Michigan	2007	1	0	0	0	1	0
Minnesota	2006	0	0	1	0	1	0
Mississippi	2011	0	0	0	0	0	0
Missouri	2009	0	0	0	1	1	1
Montana	2006	0	0	0	0	1	0
Nebraska	2006	0	1	0	1	0	0
Nevada	2005	0	0	0	0	1	0
New Hampshire	2007	0	1	0	1	1	1
New Jersey	2006	0	0	0	1	1	1
New Mexico	no SBNL	0	0	0	0	0	0
New York	2005	1	0	0	1	1	1
North Carolina	2005	0	1	0	1	1	1
North Dakota	2005	0	0	0	1	0	0
Ohio	2006	1	0	0	1	1	0
Oklahoma	2006	1	0	0	0	0	0
Oregon	2007	1	1	0	1	1	0
Pennsylvania	2006	0	0	0	0	1	0
Rhode Island	2006	0	0	1	0	0	0
South Carolina	2009	1	1	0	1	1	1
South Dakota	no SBNL	0	0	0	0	0	0
Tennessee	2005	0	1	1	0	1	0

Texas	2009	1	1	0	1	1	0
Utah	2007	1	0	0	0	0	0
Vermont	2007	0	0	1	1	1	1
Virginia	2008	1	1	1	1	1	1
Washington	2005	0	1	0	0	0	0
West Virginia	2008	1	0	0	0	1	0
Wisconsin	2007	0	0	0	1	1	0
Wyoming	2007	0	0	0	1	0	0

Appendix C – Case summaries

Case Summaries

			Breaches_per_firm			Breaches_per_firm_sel		
Sanctioning		N	Mean	Median	Std. Deviation	Mean	Median	Std. Deviation
0	2005	9	28,14	33,79	16,276	27,04	28,76	15,859
	2006	20	80,60	75,59	47,758	75,13	68,23	42,972
	2007	26	74,86	67,59	52,219	68,06	59,20	49,913
	2008	29	54,38	46,40	38,333	44,07	39,56	33,162
	2009	31	42,51	37,30	35,277	35,74	33,52	27,457
	2010	31	104,14	98,49	47,084	74,95	64,67	41,372
	2011	32	103,47	94,97	62,187	53,91	44,14	45,842
	2012	32	98,50	90,59	54,100	54,51	47,48	41,131
	Total	210	78,09	71,74	53,696	55,69	47,71	41,992
1	2005	2	14,77	14,77	10,828	14,77	14,77	10,828
	2006	7	71,94	48,79	56,674	65,18	44,14	51,392
	2007	10	71,46	77,07	34,234	58,90	53,94	33,320
	2008	12	59,89	54,10	25,060	51,17	51,38	25,790
	2009	14	50,20	50,86	27,993	42,10	41,47	30,127
	2010	14	82,76	91,98	33,940	61,63	64,43	21,441
	2011	14	91,14	89,87	29,711	52,10	50,80	29,729
	2012	14	98,43	99,15	31,208	56,13	53,42	22,322
	Total	87	74,50	74,56	36,900	53,52	53,25	29,766

Case Summaries

			Breaches_per_firm			Breaches_per_firm_sel		
Strict_Romanosky		N	Mean	Median	Std. Deviation	Mean	Median	Std. Deviation
0	2005	9	22,88	22,42	16,333	22,26	22,42	15,966
	2006	23	75,59	71,95	47,353	69,42	64,62	40,914
	2007	30	71,91	69,17	49,279	62,55	55,63	46,707
	2008	32	51,85	48,41	32,422	42,39	39,65	29,565
	2009	36	42,59	35,38	29,205	36,23	32,51	26,490
	2010	36	89,52	90,39	42,055	64,24	62,71	34,736
	2011	37	88,55	87,32	30,715	44,81	46,99	27,533
	2012	37	92,38	95,16	45,286	52,84	51,90	35,395
	Total	240	71,71	68,16	43,714	51,08	47,52	35,766
1	2005	2	38,41	38,41	,737	36,30	36,30	3,713
	2006	4	94,28	75,59	64,482	90,55	68,11	66,073
	2007	6	83,94	66,94	39,125	80,31	63,52	40,102
	2008	9	70,73	77,52	40,649	59,50	64,60	34,246
	2009	9	54,16	50,59	46,467	43,70	40,25	35,077
	2010	9	129,37	122,17	39,617	97,08	81,45	33,609
	2011	9	145,65	122,17	97,002	88,50	65,17	66,674

	2012	9	123,52	93,79	53,083	63,89	42,49	40,252
	Total	57	99,45	92,38	63,858	71,77	64,60	46,211

Case Summaries

			Breaches_per_firm			Breaches_per_firm_sel		
Private_action		N	Mean	Median	Std. Deviation	Mean	Median	Std. Deviation
0	2005	7	24,34	22,42	17,442	23,54	22,42	17,059
	2006	21	80,20	71,95	52,429	73,39	64,39	46,948
	2007	27	73,58	68,13	52,735	63,78	52,88	50,387
	2008	30	49,70	47,31	33,603	38,61	33,43	27,882
	2009	31	39,58	34,94	31,803	34,91	31,50	27,382
	2010	31	92,85	93,35	44,394	71,17	67,36	36,235
	2011	32	95,56	87,03	59,811	49,03	41,01	45,835
	2012	32	92,61	82,60	51,080	52,95	49,61	35,223
	Total	211	73,27	66,51	51,292	52,79	46,99	40,525
1	2005	4	28,09	33,32	14,920	27,04	31,22	14,126
	2006	6	71,89	81,79	39,238	69,63	78,33	38,201
	2007	9	74,92	70,11	28,470	70,71	66,83	28,604
	2008	11	73,16	77,52	33,369	66,70	62,43	31,053
	2009	14	56,69	55,27	33,879	43,94	50,53	29,777
	2010	14	107,77	101,05	43,514	70,00	63,50	38,858
	2011	14	109,24	112,81	39,339	63,24	64,92	27,141
	2012	14	111,88	96,83	38,122	59,68	50,45	39,269
	Total	86	86,29	88,88	43,066	60,61	60,39	33,680

Case Summaries

			Breaches_per_firm			Breaches_per_firm_sel		
Scope_law		N	Mean	Median	Std. Deviation	Mean	Median	Std. Deviation
0	2005	5	28,25	38,93	19,699	28,25	38,93	19,699
	2006	17	81,00	72,44	51,076	73,41	64,39	45,103
	2007	21	76,51	66,83	56,041	66,14	53,07	54,142
	2008	23	54,20	48,22	38,688	42,48	39,56	32,669
	2009	23	47,32	40,25	36,535	39,52	34,37	31,926
	2010	22	96,50	86,97	49,694	70,06	63,47	35,104
	2011	22	93,82	90,39	35,995	44,98	38,11	37,475
	2012	22	102,90	96,06	45,699	55,51	53,23	26,656
	Total	155	76,84	71,45	48,688	54,30	47,75	39,239
1	2005	6	23,59	25,59	13,545	21,95	25,29	11,961
	2006	10	73,87	75,35	48,232	71,09	68,23	45,781
	2007	15	70,29	70,11	33,436	64,63	70,11	31,886
	2008	18	58,29	52,96	29,914	50,83	45,35	29,057
	2009	22	42,38	36,56	29,641	35,84	34,23	24,132
	2010	23	98,43	100,49	39,305	71,52	67,89	38,807
	2011	24	105,13	94,97	67,297	61,04	56,22	43,844
	2012	24	94,42	93,09	50,522	54,53	47,49	43,746
	Total	142	77,25	74,70	50,207	55,87	51,78	38,383

Case Summaries

			Breaches_per_firm			Breaches_per_firm_sel		
Not_ag		N	Mean	Median	Std. Deviation	Mean	Median	Std. Deviation
0	2005	8	24,21	26,22	18,294	23,51	23,41	17,978
	2006	18	80,76	68,53	50,557	74,54	64,51	44,935
	2007	24	60,51	61,54	43,341	53,02	48,12	43,589
	2008	26	53,23	47,31	33,214	42,85	37,95	29,219
	2009	28	39,08	34,67	26,684	33,87	32,51	25,060
	2010	28	96,06	94,97	41,505	67,09	63,37	33,380
	2011	29	86,28	90,91	30,020	37,50	35,49	25,937
	2012	29	92,85	95,16	50,118	54,49	51,90	37,422
	Total	190	70,86	66,53	44,525	49,53	46,84	36,023
1	2005	3	29,69	28,76	7,772	28,29	28,76	5,640
	2006	9	73,54	78,74	49,029	68,58	67,71	45,969
	2007	12	100,73	93,58	45,380	90,51	83,20	40,381
	2008	15	60,79	54,06	37,972	51,86	48,60	34,247
	2009	17	54,48	49,86	40,587	44,07	36,26	32,354
	2010	17	99,85	99,13	49,514	76,92	72,10	41,778
	2011	17	122,65	111,52	76,418	80,41	65,17	48,798
	2012	17	108,07	93,79	43,718	55,87	39,40	35,103
	Total	107	88,01	84,63	55,428	64,86	60,13	41,628

Case Summaries

			Breaches_per_firm			Breaches_per_firm_sel		
Not_custcredit		N	Mean	Median	Std. Deviation	Mean	Median	Std. Deviation
0	2005	5	22,16	18,65	20,170	21,31	18,65	19,424
	2006	12	79,02	67,90	62,940	73,00	58,74	56,735
	2007	15	65,25	67,05	60,516	54,92	39,07	55,966
	2008	16	45,06	43,47	34,451	34,55	38,60	25,380
	2009	16	33,17	32,95	23,921	30,11	29,09	25,651
	2010	16	100,44	109,18	49,855	72,68	67,75	41,026
	2011	17	85,81	86,75	36,591	40,26	35,49	33,801
	2012	17	92,26	95,30	61,631	44,50	47,32	33,254
	Total	114	69,51	55,69	52,733	47,76	40,77	41,251
1	2005	6	28,66	31,28	12,539	27,72	28,46	12,287
	2006	15	77,82	72,44	37,235	72,19	64,62	33,841
	2007	21	80,10	68,24	35,778	73,08	66,83	36,155
	2008	25	62,99	54,15	33,770	53,57	51,86	32,496
	2009	29	51,37	50,59	35,902	41,92	36,14	28,970
	2010	29	95,86	87,43	41,572	69,77	64,67	34,692
	2011	29	107,88	95,37	61,586	61,04	50,92	43,819
	2012	29	102,12	93,79	38,533	61,16	53,25	36,975

Total	183	81,73	77,52	46,633	59,59	53,29	36,533

Appendix D – Cost of compliance and non-compliance

In section 4.3.1, the cost of compliance and non-compliance are estimated as follows:

Expected cost of compliance and non-compliance per breach

- Cost of compliance (reputational damage)
  - European Union: 500000 dollar
  - Michigan: 500000 dollar
- Cost of non-compliance (possible reputational damage and possible penalty)
  - European Union: 210000 dollar
  - Michigan: 375000 dollar

This is done by making the following assumptions.

- Worldwide turnover: 10 million dollar
- Price to sales ratio: 5:1
- Market value (worldwide turnover*price to sales ratio) = 50 million dollar
- Likelihood of apprehension: 10%
- Likelihood of unintended disclosure: 20%
- Michigan fine: 750000 dollar
- European Union fine: 2% of worldwide turnover.
- Reputation damage: 1% loss of market value

The cost of compliance in Michigan and the European Union equals the reputation damage. The reputation damage = 1% * market value = 1% * 50 million dollar = 500.000 dollar.

The cost of non-compliance equals the expected value of the sanction and the reputation damage. The sanction in the European Union = 2% * worldwide turnover = 2% * 10 million dollar = 200000 dollar. The likelihood of 'getting caught' = Likelihood of apprehension + likelihood of unintended disclosure = 10% + 20% = 30%. Thus the expected value of the cost of non-compliance = likelihood of getting caught * (sanctioning + reputation damage). In the European Union this equals 30% * (200000 dollar + 500000 dollar) = 210000 dollar. In Michigan this equals 30% * (750000 dollar + 500000 dollar) = 375000 dollar.