An Analysis of the Effectiveness of the EU Data Breach Notification Obligation

Bernold Nieuwesteeg [a*] ***and Michael Faure*** [b]

[a] *Erasmus University Rotterdam, The Netherlands*
[b] *Erasmus University Rotterdam and Maastricht University, The Netherlands*

ABSTRACT

In this paper we study the law and economics of the EU data breach notification obligation (EU DBNO), which is part of the General Data Protection Regulation. We start our discussion with the origins and aims of the EU DBNO. Following this, we study the social benefits of the DBNO and the conditions for these social benefits to emerge. Next, we analyse whether there would be spontaneous notification without the existence of a DBNO. We discuss how the national DPAs, that are responsible for the execution of the EU DBNO, can sufficiently induce data controllers to comply with the regulation. We also discuss the scope of the regulation from a social welfare perspective, in particular the conditions, which trigger a notification from data controllers.

Keywords: Data breach notification obligation; GDPR; social welfare analysis; data protection authority; deterrence; disclosure threshold; digital first aid kit

1. Introduction

At November 7 2016, the Erasmus University Rotterdam experienced a large data breach affecting 17,000 individuals.[1] The data breach was notified to the Dutch Data Protection Agency (DPA) and to the individuals affected.[2] We were also affected and notified and experienced the practical effects of data breach disclosure. This paper will perform a law and economics analysis on the European Union data breach notification obligation (Hereafter 'EU DBNO' or 'the DBNO') as incorporated in Articles 33 and 34 of the General Data Protection Regulation

* Corresponding author. Address: Burgemeester Oudlaan 50, 3062 PA, Rotterdam, The Netherlands. Email address: nieuwesteeg@law.eur.nl (B.F.H. Nieuwesteeg).

[1] See JP Buntinx, 'Erasmus University Data Breach Exposes Students' Medical and Financial Information' (*The Merkle,* 30 November 2016) <https://themerkle.com/erasmus-university-data-breach-exposes-students-medical-and-financial-information/> accessed 16 May 2018.

[2] The Dutch Data Protection Authority is called the Autoriteit Persoonsgegevens, see <www.autoriteitpersoonsgegevens.nl> accessed 16 May 2018.

Regulation 2016/679, hereafter: GDPR).[3] The EU DBNO imposes an obligation on organizations to disclose certain breaches of personal data to a notification authority and to affected individuals (hereafter: data subjects). We will analyse whether the EU DBNO is effective in increasing social welfare. In addition, we will propose recommendations for the ex post execution and enforcement of this important piece of legislation.[4]

Our core methodology will be a law and economics analysis of incentives and optimal enforcement.[5] Unfortunately, there is little empirical research available, especially on the EU DBNO, since at the time of conducting this research, the EU DBNO did not yet apply and hence no data breach data had been generated. Moreover, there is no reliable data, for example concerning the effects of obligations to disclose breaches of personal data in the EU. The entire EU DBNO is therefore largely based on assumptions on how data controllers will react to the DBNO, given the particular sanctioning regime. Even theoretically, it is difficult to predict the effects of the regime as it strongly depends on specific assumptions. While our contribution aims to explain and analyse the various effects of the EU DBNO, we will also state when we make these specific assumptions. In addition, we will utilize the literature on the effectiveness of DBNOs in the US. In the US, most states have a DBNO and consequently there is empirical research regarding the data breach notifications.[6] This stream of literature has covered regulatory impact,[7] effectiveness in reducing identity theft,[8] economic effects,[9] perceptions from the private sector[10] and the need to integrate the US state level laws into a federal law.[11]

---

[3] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/1.
[4] Those breaches of personal data can be both analogue and digital. In practice, losses of personal data are mostly occurring within a digital infrastructure, because the majority of personal data records is stored online in our digitalized society. In this paper we will primarily focus on personal data breaches in the digital society.
[5] See in this respect also A. Mitchell Polinsky and Steven Shavell, *Handbook of Law and Economics* (vol. 1, 1st edn, Elsevier 2007) chapter 6.
[6] See <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx> (accessed 16 May 2018) for a brief overview regarding the legislative status of US DBNOs.
[7] Jane Winn, 'Are "Better" Security Breach Notification Laws Possible?' (2009) 24 Berkeley Technology Law Journal 1133.
[8] Sasha Romanosky, Rahul Telang and Alessandro Acquisiti, 'Do Data Breach Disclosure Laws Reduce Identity Theft?' (2011) 30 Journal of Policy Analysis and Management 256.
[9] Thomas Lenard and Paul Rubin, 'Much Ado About Notification' (2016) 29 Regulation 44; Stefan Laube and Rainer Böhme, 'The economics of mandatory security breach reporting to authorities' (2016) 2 Journal of Cybersecurity 29, uses a theoretical model and also involves EU law.
[10] Deirdre Mulligan and Fred Schneider, 'Doctrine for Cybersecurity' (2011) 140 Daedalus 70.
[11] Fabio Bisogni, 'Proving Limits of State Data Breach Notification Laws: Is a Federal Law the Most Adequate Solution?' (2016) 6 Journal of Information Policy 154.

To the best of our knowledge, a law and economics analysis of the new DBNO in the European Union has not yet been performed.[12] A thorough (ex ante and ex post) scrutiny of the effects of the DBNO contributes to the development of EU law and implementing EU data protection policy.[13]

This paper is structured as follows. In section 2, we introduce the EU DBNO, its origins, aims and its embedded position in the General Data Protection Regulation. We also discuss other breach notification obligations in the EU and compare the EU DBNO with state level DBNOs in the US. In section 3, we discuss the social costs and benefits of the DBNO relative to the threshold of notification. Section 4 discusses whether organizations would have sufficient incentives to notify, in the absence of the regulation. We discuss the reasons to believe that these incentives are likely to be insufficient and conclude that a market failure is likely to exist in the absence of regulation. In section 5, we discuss whether and in which cases the DBNO is justified in correcting this market failure. In doing so, we also take the public costs of the regulation into account. In section 6, we continue our discussion by analysing whether the current legislative design of the upcoming DBNO is capable of inducing organizations to notify at an acceptable social cost. The section discusses several socially ideal design choices for optimizing the social potential of the DBNO and compares them with the actual choices made by the EU legislator. We will also discuss incentive schemes related to the implementation of the DBNO that the EU legislator did not include in the actual text of the DBNO, such as rewarding compliance and the enforcement of sanctions. Section 7 discusses the optimal notification threshold for both Article 33 (notification to the DPA) and Article 34 (notification to data subjects) and section 8 will provide some concluding remarks.

2. The European Union Data Breach Notification Obligation

This section will start by briefly introducing the origins and specific characteristics of the EU DBNO in section 2.1. Section 2.2 will shortly discuss other EU DBNOs currently in force in the EU, which mostly concern a certain sector or topic. As stated in the introduction, the study utilizes the literature on the effectiveness of DBNOs in the US. In the US, most states have a DBNO and consequently there is empirical research regarding the data breach notifications.[14] Section 2.3 discusses the similarities and differences between the EU and US DBNO regimes.

---

[12] Such an analysis did not take place at a Member State level either. Some EU countries, such as Germany, Ireland, Italy, Lithuania, Luxemburg, Malta and the Netherlands independently adopted a DBNO before the entry into force of the GDPR.

[13] The only research we are aware of scrutinizing the EU DBNO is from Paul de Hert and Vagelis Papakonstantinou, 'The new General Data Protection Regulation: Still a sound system for the protection of individuals?' (2016) 32 Computer Law and Security Review 179, 191, who take a more legal approach.

[14] Op. cit. NCSL.org (n 6).

2.1. The DBNO in the GDPR

The DBNO is part of the extensive legislative data protection package known as the General Data Protection Regulation abbreviated as GDPR. The GDPR regulates many aspects related to the processing of personal data such as basic principles (Article 5), lawfulness of processing and individual consent (Article 6) and rights of individuals that have provided their data to a third party (section 2 of the GDPR). The GDPR entered into force on May 24 2016 and applies after a two-year transition period from May 25 2018.[15] Contrary to its predecessor, Directive 95/46/EC,[16] the GDPR will equally apply directly to every citizen and organization falling within the scope of European Union law.[17] Hence, the GDPR will be an influential piece of legislation. The GDPR provides for the DBNO in Articles 2(2), 4(7), 4(12), 33, 34 and 83(4):

Article 4 (12) defines a personal data breach as 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'. The definition thus focuses on the consequences of the data breach. In doing so, the EU legislator incorporates the 'CIA triad' of confidentiality, integrity or availability of personal data.[18] Possible differences in the origin of the data breach, for instance whether a data breach is intentional or negligent, are not relevant for defining a data breach.

Articles 4 (7) states which entities have to notify data breaches. These 'data controllers' can be legal persons or public authorities. Hence, the DBNO applies to both public and private organisations.

Article 2 (2) excludes certain data breaches from the notification duty. Data that (a) falls outside the scope of EU law; (b) falls within the scope of Chapter 2 of Title V of the TEU; (c) is carried out by a natural person for personal use or (most notably) (d) is used for the execution of criminal prosecution do not have to be notified when breached.

Articles 33 and 34 regulate the actual obligation to disclose a data breach.[19] There is an apparent difference in notifying a data breach to a data protection authority (DPA, Article 33) or to the data subjects affected (Article 34). With respect to the former, a data controller has to notify the DPA 'unless the personal data breach is *unlikely* to result in a risk to the rights and freedoms of natural

---

[15] GDPR, Art. 99.
[16] Directive 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 L281/31 (Data Protection Directive).
[17] Directive 95/46/EC (Data Protection Directive) did not contain a requirement to notify data breaches.
[18] Shari L. Pfleeger, 'A Framework for Security Requirements' (1991) 10 Computers & Security 515, 518.
[19] Of less importance for this paper it the obligation under Article 33 (2) which states that data processors, which process data on behalf of the controller, have the obligation to notify the controller without undue delay after becoming aware of a personal data breach.

persons'.[20] Hence, this 'likelihood' is the key threshold for notifying the DPA. Article 33(1) further specifies that the notification should be as soon as possible, and not later than 72 hours after the data breach. However, this is apparently not a red line, because if it is not feasible to do so, the organization can notify later, but has to specify the reasons why it does so. Under 33(3), the data controller has to include the nature of the breach, its consequences for data subjects, a description of counter-measures undertaken and a contact point. When possible, the organization should also include the type and number of affected data subjects and the amount of records, which have been breached.

Article 34 shows that the threshold for mandatory notification to data subjects is higher on several points compared to the requirements for notifying the DPA ex Article 33. First, notification to data subjects is only mandatory when the data breach is 'likely to result in a *high* risk to the rights and freedoms' of data subjects. Hence, where in Article 33 a certain risk suffices, in the case of Article 34 the risk should be high. The GDPR does not specify this gap between risk and high risk any further.[21] Concerning the temporality of notification, Article 34(1) solely determines that this should be without undue delay and does not specify the 72 hours of Article 33. In addition, the organization does not have to describe the nature of the data breach and the amount of data subjects affected when notifying data subjects. Article 34(3) heightens the threshold even further. This Article provides three possible arguments that organizations can use not to communicate to data subjects. First, organizations may refrain from notifying data subjects when the data is made sufficiently difficult to use, for instance with encryption.[22] Second, when the organization has taken 'subsequent measures', which ensure that the high risk will no longer materialize, they do not need to notify. Third, notification to data subjects is not necessary when it would lay a disproportionate burden on the organization. Ergo, there is quite a large difference in the execution of notification to the DPA and to the data subject. The GDPR does not state the reasons for this difference. However, Article 34(4) regulates that the DPA may require the organization to still issue an additional notification to data subjects when the DPA assesses that the likelihood of adverse consequences for data subjects is 'high' according to Article 34(1).

Article 83(4) states that a sanction of €10,000,000 or 2% of the undertakings turnover, whichever is higher, can be imposed when the data controller fails to notify a data breach.[23] These sanctions

---

[20] As such, it is quite peculiar that the Article speaks of a likelihood *to result in* a risk, since risk also contains the element of likelihood. (risk = likelihood * impact). Hence, within this paper, we will just use the term risk.
[21] Op. cit. De Hert and Papakonstantinou (n 13) 191.
[22] The topic of encryption and DBNOs, although not in the context of the GDPR, is extensively discussed by Mark Burdon, Jason Reid and Rouhshi Low, 'Encryption safe harbours and data breach notification laws' (2010) 26 Computer Law & Security Review 520.
[23] GDPR, Art. 83(4); GDPR, Art. 83(2) specifies guidelines for the determination of the actual magnitude of the sanction.

are high compared to the sanctions in the US, whereby state level DBNOs usually have sanctions in the magnitude of $100,000s or lower.[24]

The de jure text of the DBNO is definite and will not change in the near future.[25] However, the ex post execution and enforcement of the obligation will necessitate a combination of knowledge regarding EU law, data security and regulatory enforcement. Therefore, we believe that the upcoming social welfare analysis contributes to the development of EU law and policy after the entry into force of the regulation.

2.2. Other notification duties of data breaches currently in force in the EU

The EU DBNO in the GDPR is not the only notification duty that currently applies in the EU.[26] In addition, on a Member State level, there are often many more DBNOs, which could overlap or be replaced by the EU DBNO. In this section, we will limit ourselves by discussing DBNOs that could entail personal data on an EU level.

Article 4(3) E-privacy directive 2009/136/EG amending directive 2002/58/EC regulates a data breach notification obligation for telecommunication providers. The wording of the DBNO in the GDPR has similarities with this directive since it states that '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 adversely to 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'. Commission Regulation 611/2013 further regulates the details of data breach disclosure in the context of the E-privacy directive. The E-privacy directive and the GDPR are not mutually exclusive, since telecommunication providers also fall within the scope of the GDPR. However, on some elements, the data breach disclosure requirements for telecommunication providers are somewhat stricter. For instance, the data breach has (when feasible) to be notified within 24 hours (Article 2(2) Regulation 611/2013) compared to the 72 hours that are required in Articles 33 and 34 of the GDPR.

Article 19(2) eIDAS Regulation 910/2014 regulates the mandatory disclosure of a breach of security or the loss of integrity of trust services providers such as certificate authorities. These

---

[24] Bernold Nieuwesteeg, *The Legal Position and Societal Effects of Security Breach Notification Laws* (1st edn, deLex 2014) 80.
[25] After all, there have been more than two decades in between the entry into force of Regulation 2016/679, and its predecessor, Directive 95/46/EC.
[26] For a more extensive, albeit slightly out-dated overview (since it discusses the draft-GDPR and proposed NIS-directive), we refer to Samson Esayes, 'Breach Notification Requirements Under the European Union Legal Framework: Convergence, Conflicts, and Complexity in Compliance' (2014) 31 J. Marshall J. Info. Tech. & Privacy L. 317.

losses could also entail the loss of personal data, and insofar the breach or loss of integrity adversely affects a natural or legal person this person should also be notified.[27]

Article 30 and Article 31 EU directive 2016/680 on the processing of personal data by competent authorities. Parallel to the legislative process GDPR, a directive was drafted that regulates data processing for competent authorities, such as the judicial apparatus of EU Member States. This directive also regulates data breach disclosure by these competent authorities to the supervisory authority (Article 30) and the data subject (Article 31). One of the main other differences with the GDPR is that Member States are free to implement a sanctioning system as long as this is 'effective, proportionate and dissuasive' (Article 57).

Article 14 (3) NIS (network and information security) Directive 2016/1148. The NIS directive regulates cyber security for network and information systems, which are 'essential services' such as the energy and utility industry. Article 14 (3) regulates the security breach notification. Operators of essential services should, without undue delay, incidents having a significant impact on the continuity of the essential services they provide to a competent authority.[28] These incidents, such as for instance a cyber-attack on a power grid, could also entail personal data breaches, although one could expect that these companies would separately disclose these data breaches under the GDPR or E-privacy directive regime.

2.3. Differences between the EU and US legislation

There are significant differences between the DBNO regimes in the EU and US. Firstly, the EU DBNO is regulated at a central European level instead of at the state level for US laws, which are partly much older than the EU law.[29] California was the first US state to adopt a DBNO in 2006 and other states quickly followed.[30] As of March 28, 2018, Alabama became the 50th and final state to enact a DBNO.[31] This patchwork of state level DBNOs has provided some challenges. For instance, large (national) data breaches that involve records of data subjects in multiples states have to be notified according to the various (slightly different) legal regimes.[32] Therefore,

---

[27] See for a discussion of the topic: Axel Arnbak, Hadi Asghari, Michel van Eeten and Nico van Eijk, 'Security collapse in the HTTPS market' (2014) 57 Communications of the ACM 47.
[28] Which is (often) a different authority than the data protection authority of the GDPR.
[29] Ibid 155.
[30] Op. Cit. Nieuwesteeg (n 24).
[31] Aleksandra Vold, 'That's All Folks! Alabama Becomes 50th State With Breach Notification Law' (*Thompson Coburn LLP,* 11 April 2018) <https://www.thompsoncoburn.com/insights/blogs/cybersecurity-bits-and-bytes/post/2018-04-11/that-s-all-folks!-alabama-becomes-50th-state-with-breach-notification-law> accessed 16 May 2018.
[32] For instance, the thresholds and legal language between the US state level DBNOs differ. See Mark Burdon, Bill Lane and Paul von Nessen, 'The mandatory notification of data breaches: Issues arising for Australian and EU legal developments' (2010) 26 Computer Law & Security Review 115.

there has been some literature regarding the desirability of a DBNO on a central level in the US.[33] We will not include this stream of literature in our main argument because the patchwork issue is not relevant in the EU since the DBNO is regulated at a central level.

Secondly, concerning the sanctioning regime, which is one of the corner stones for our law and economics analysis, there are also some notable differences. In the US, the administrative penalties for DBNOs are usually two orders of magnitude lower than in the EU DBNO. For instance, the Virginia data breach notification law, which has one of the highest sanctions in the US, allows for an imposition of a $150,000 fine.[34] However, in the US, privacy class actions could be a much more significant cost for organizations.[35]

Thirdly, the main *reason d'être* of the US and EU DBNO is different. Section 3.2 will show that there are three social benefits for DBNOs: the right to know for data subjects that data is lost or harmed, information diffusion regarding data breaches and the possibility to claim damages by these same data subjects. For the European Union, the protection of personal data and the right to know has been the primary reason to adopt the EU DBNO since it is part of the General *Data Protection* Regulation. In the US, the multitude of the three social benefits, especially the right to know and information diffusion, are positioned more equally.[36]

Hence, we will take the peculiarities of the EU legal regime into account in order to facilitate transplantation of the lessons learned on the other side of the Atlantic. For instance, in pursuing the social benefit of information diffusion in the EU DBNO, one should be cognizant of the fact that information diffusion about personal data breaches and mutual learning has not been the main starting point of the legislative process that has led to the GDPR and the DBNO.

3. The social benefits and costs of the DBNO

This section discusses the social benefits of the DBNO generally. The starting point here is that the social benefits of the DBNO depend on the disclosure threshold. Section 3.1 will further introduce this 'threshold' perspective. Section 3.2 will discuss the social benefits of a DBNO, while section 3.3 will discuss its social costs.

---

[33] See for instance: Fabio Bisogni, 'Proving Limits of State Data Breach Notification Laws: Is a Federal Law the Most Adequate Solution' (2016) 6 Journal of Information Policy 154.

[34] Code of Virginia §18.2-186.6.

[35] Sasha Romanosky, David Hoffman and Alessandro Acquisti, 'Empirical Analysis of Data Breach Litigation' (2014) 11 Journal of Empirical Legal Studies 74.

[36] Op. cit. Romanosky, Telang and Acquisti (n 8) 258.

3.1. The threshold

The EU legislator defines the data breach notification threshold in the GDPR: data breaches that result in a 'risk to the rights and freedoms of natural persons' in the case of notifying the DPA (Article 33). In the case of notification to affected data subjects, this risk should be 'high' (Article 34). Naturally, some data breaches are more risky than others are.[37] Identity theft has a high risk, credit card theft has a lower risk and the theft of certain passwords and usernames of non-vital websites, as well as encrypted data, have an even lower risk.[38] Hence, theoretically, these data breaches can be plotted on a risk continuum. The two thresholds within the EU DBNO are certain points on this risk continuum. This paper discusses to what extent the social outcomes of the regulation change when the risk threshold is interpreted more or less strictly and consequently more or fewer data breaches have to be notified. To be precise, we will observe the drivers for a change in private and social optima when the threshold shifts.[39] In section 7, we will also discuss whether it is socially desirable to distinguish between thresholds for notifying to the DPA and to the data subjects affected. In the upcoming sections, we will primarily focus on the private and social benefits and costs of notification to data subjects ex Article 34 GDPR. In section 7.1 we will address the different situation of the obligation to notify the DPA.

3.2. The social benefits

This section will discuss the social benefits of data breach disclosure to data subjects. First, and foremost for the GDPR , the social benefit of data breach disclosure is the implementation of the data subjects' 'right to know' that their data has been compromised. This 'right to know' is an aspect of the fundamental right on the protection of personal data, enshrined in the Charter of Fundamental Rights of the European Union and the European Convention of Human Rights.[40] The protection of personal data has been the primary reason for the European Union to adopt the GDPR and therein the EU DBNO.[41] The social benefit of the 'right to know' is intangible. In addition, its intrinsic value varies among schools of thought. On one side of the spectrum, there is

---

[37] This paper does not aim to provide an extensive overview of personal data breaches and their risk for individuals, organizations and society. For the potential consequences of personal data breaches and their risks for individuals and organizations see inter alia Verizon, 'Data Breach Investigations Report' <http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/> accessed 16 May 2018,

[38] GDPR, Art. 33(3) under c; Compare for instance the Steam hack which also included credit card theft, but also less vital username information: Casey Johnston, 'Valve confirms Steam hack: credit cards, personal info may be stolen' (*Ars Technica,* 11 November 2011) <https://arstechnica.com/gaming/2011/11/valve-confirms-steam-hack-credit-cards-personal-info-may-be-stolen/> accessed 16 May 2018.

[39] We assume that data breaches carry a similar amount of records (being affected consumers).

[40] Charter of Fundamental Rights of the European Union [2012] OJ C 326/1, Art. 8; European Convention of Human Rights, Art. 7. The right to know is described clearly in Article 8(2) of the Charter, which states that "everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified".

[41] GDPR, Art. 1.

a stream of literature that prioritizes fundamental rights by qualifying it as 'a first line of defence'.[42] On the other side of the spectrum, there is literature that argues that the right to know has a limited value,[43] supported by empirical research that evaluates the low monetary value consumers attach to this right.[44] The valuation of the right to know will, in a democratic society, be decided by the policy-maker according to the preferences of the voter. In addition, the value of the right to know will strongly depend upon the nature of the data breach. For example, it may be more important for an individual to be aware of an identity theft than of the loss of a username or password for a Steam account (a platform for mobile gaming).[45]

Second, data breach disclosure will result in additional incentives for data security improvements for individuals and organizations. There are short and long-term effects and direct and indirect effects of the diffusion of data breach disclosure information.[46] Data breach disclosure has a short- term direct impact on mitigating and avoiding consumer[47] and organizational losses.[48] However, organizations and individuals may over-invest in their security improvements.[49] In the long term, according to US chief security officers, data breach disclosure can foster "cooperation between information security departments".[50] This diffusion of information has positive effects on overall security.[51] Furthermore, indirectly, a data breach disclosure raises the public's awareness regarding cyber security. Similar to the right to know, we assume that the information benefit for security improvement is lower when the significance of the data breach risk is lower.

---

[42] Axel Arnbak, *Securing private communications: protecting private communications security in EU law - fundamental rights, functional value chains, and market incentives* (1st edn, Kluwer Law International 2016) Chapter 4.
[43] Richard Posner, *Economic Analysis of Law* (6th edn, Aspen Law & Business 2002) 711.
[44] Ignacio Cofone, 'The Value of Privacy: Keeping the Money Where the Mouth is' (2014) RILE Working Paper Series 15/2014, <http://www.econinfosec.org/archive/weis2015/papers/WEIS_2015_cofone.pdf> accessed 16 May 2018.
[45] This gradual decrease occurs independently of the absolute value of the right to know, which, as said, has to be determined by societal debate.
[46] Op. cit. Romanosky, Telang and Acquisiti (n 8) 259; This is also the aim of the Dutch DBNO which states in its explanatory memorandum that the central availability of the information will stimulate the ability to learn of organizations which have been breached.
[47] Paul Schwartz and Edward Janger, 'Notification of Data Security Breaches' (2007) 105 Michigan Law Review 913, 915; Deirdre Mulligan, *Security Breach Notification Laws: Views from Chief Security Officer* (Study Conducted for the Samuelson Law, Technology & Public Policy Clinic, University of California-Berkeley School of Law, 2007) 23, available through <https://www.law.berkeley.edu/files/cso_study.pdf> accessed 16 May 2018. This discussion is linked to the timing of the notification studied by Fabio Bisogni, 'Data Breaches and the Dilemmas in Notifying Customers' (2015), presented at The fourteenth Annual Workshop on the Economics of Information Security, Delft, 22-23 June 2015. The faster the disclosure takes place, the more benefits for consumers. We expect this to be equal over significance.
[48] Op. cit. Romanosky, Telang and Acquisti (n 8) 258.
[49] Op. cit. Lenard and Rubin (n 9) 48.
[50] Op. cit. Mulligan (n 47) 18.
[51] Hulisi Ogut, Srinivasan Raghunathan and Nirup M. Menon, 'Information Security Risk Management through Self-Protection and Insurance' (2005) The University of Texas School of Management 1, 31.

Third, the potential liability claim that can follow a disclosure has a social benefit. Liability results in behaviour that incentivizes organizations to internalize some of the externalities in cyber security. Quite naturally, individuals can only claim damages when a data breach disclosure becomes public and they are aware of it. Liability can even accumulate in class actions.[52]

3.3. The social costs

There are also social costs of data breach disclosure. First, individuals and organizations whose data have been breached incur direct costs because they have to spend time and money in order to analyse and mitigate their impact. This might be a minor cost per record, but if hundreds of thousands of records are being breached, the numbers quickly add up.[53] The cost of consumer actions might be greater than expected because consumers can spend several hours of time on their accounts and impose costs on firms by requesting more information on, for instance, new credit cards. Lenard and Rubin estimate that this cost is $10 per data subject.[54] Second, an increase in the amount of notifications can lead to a decrease in the positive effects of disclosure, because data subjects can pay less attention to each individual data breach. Subsequently, the information diffusion becomes less meaningful and eventually all data breaches could just be perceived as irrelevant information.[55] We label this effect 'notification fatigue'. Thus, notification fatigue does not only affect the benefits of the (least important) data breach, but also has negative externalities towards other data breaches. All data breaches become less important with the introduction of an additional data breach (through lowering the threshold). Likewise, as soon as more notifications are being made, for example by lowering the notification threshold, the benefits of the additional data breach will decrease and the costs (the negative externality to other data breaches) will increase. Third, organizations may over-invest in security because of notifying the data breach. However, this is not expected to be a very significant social cost because in general, organizations have incentives to under-invest in cyber security.[56]

3.4 Social costs versus social benefits

Table 1 below displays the social costs and benefits relative to a decreasing notification threshold.

Table 1: Social costs and benefits

---

[52] Especially in the US, see op. cit. Romanosky, Hoffman and Acquisti (n 8).
[53] For instance a consumer spends 10 minutes on gaining knowledge about a data breach, at an 18 euro per hour opportunity cost, a 100.000 record breach can costs society 300.000 euro. These costs are public costs insofar as they are not being compensated by the private organization.
[54] Op. cit. Lenard and Rubin (n 9) 47. It is more likely to be on the upper side of the spectrum.
[55] Op. cit. Mulligan (n 47) 33.
[56] Due to the mainly positive externalities that are present in cyber security.

Social benefits	Marginal social benefits relative to a decreasing notification threshold	Social costs	Marginal social costs relative to a decreasing notification threshold
Right to know	Decreasing	Administrative costs (data subject side)	Minor decrease
Information diffusion	Decreasing	Notification fatigue	Increasing
Liability	Decreasing	Over-reaction in restricting security	Decreasing

Marginal social benefits all decrease when less risky data breaches have to be notified. The marginal administrative cost is likely to decrease, because the data subject will take more time in reviewing a risky data breach than a less risky data breach. However, the decrease will quickly flatten out, because a certain base line of investigative costs have to be made by each data subject. In addition, over-investment by organizations will be less likely when less important data breaches have to be notified. Notification fatigue will logically strongly increase when a larger pool of data breaches have to be notified. Notification fatigue drives overall marginal social costs to increase and the minor decrease of administrative cost and the overall minor decreasing effect of over-investment cannot compensate for that. In sum: there may be positive social benefits from notification, but these can be reduced because of notification fatigue. To reduce that risk, determining the appropriate threshold for notification is crucial (see section 7). For now, we assume that a smart threshold will be determined and that disclosure is therefore socially beneficial. That then leads to the following question:

4. Will there be spontaneous disclosure in the absence of the obligation?

This section discusses whether there will be spontaneous disclosure in the absence of the obligation. We will assess the private costs and benefits because of disclosure. Section 4.1 will discuss private benefits and section 4.2 will discuss private costs. Section 4.3 will balance these costs with these benefits.

4.1. Private benefits

First, organizations experience a benefit because the disclosure of data breaches allows for the faster mitigation of the impact of the breach. This reduces direct costs. This is especially relevant when consumers need to take action after the data breach, such as refraining from using stolen credit card information or using old passwords. Moreover, a DPA can potentially assist in mitigating the breach by providing targeted advice.

4.2. Private costs

Besides benefits, private parties also incur costs when disclosing data breaches.[57] First, there are the administrative costs of disclosing data breaches to the affected data subjects. However, the major risk is (perceived) reputation damage. The literature shows that data breach disclosure does have limited single digit (1 or 2%) negative market value impact on the short term.[58] However, research that focussed on the long term suggests, "information security breaches have minimal long-term economic impact".[59] We believe that the Target stock price example shows the difficulty in pointing out long-term reputational damage. Target was the subject of a very significant data breach in December 2013. Figure 1 below displays the graph of the stock market value of Target. It is impossible to identify the day of the data breach, as on other trading days stock prices did fluctuate more than during the event in late December. [60]

---

[57] These private costs, and the necessity to balance these costs with the social benefits of DBNOs have been debated in the literature. For instance, Mark Burdon, Bill Lane and Paul von Nessen, 'Data breach notification law in the EU and Australia – Where to now?' (2012) 28 Computer Law & Security Review 296, 307 mention competing rationales, such as the 'dual conflict of effective consumer protections relating to identity theft threats and minimising corporate compliance costs.'

[58] Reputation damage is usually quantified as the difference in company value before and after the disclosure. Sanjay Goel and Hany Hawsky, 'Estimating the market impact of security breach announcements on firm values' (2009) 46 Information & Management 404, 408, used such an event study methodology. They measured the market value of the company a few days before and after the notion of a security breach and found a negative effect of on average about 1% of the market value. Huseyin Cavusoglu, Birendra Mishra and Srinivasan Raghunathan, 'The Effect of Internet Security Breach Announcement on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers' (2004) 9 International Journal of Electronic Commerce 69, 71, identified through a similar approach an incidental loss of stock prices of 2.1%. They discuss direct and indirect costs of data breaches, but this is a slightly different topic, as this paper is about to talk about data breach disclosure. Pierangelo Rosati, Mark Cummins, Peter Deeney, Fabian Gogolin, Lisa van der Werff and Theo Lynn, 'The effect of data breach announcements beyond the stock price: Empirical evidence on market activity' (2017) 49 International Review of Financial Analysis 146, 152, find that market activity on the short term slightly higher after a data breach announcement.

[59] Myung Ko and Carlos Dorantes, 'The impact of information security breaches on financial performance of the breached firms: an empirical investigation' (2006) 16 Journal of Information Technology Management 13, 20, used a matched sample comparison analysis instead of event study methodology to investigate the impact of security breaches on firm performance. These observations about long-term impact should be taken with care, because the effect of the data breach is much harder to disentangle from other exogenous variables and high quality panel data is not available.

[60] 'In the days prior to Thanksgiving 2013, someone installed malware in Target's security and payments system designed to steal every credit card used at the company's 1,797 U.S. stores.' See Michael Riley, Ben Elgin, Dune Lawrence and Carol Matlack, 'Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It' (*Bloomberg,* 17 March 2014) <https://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data> accessed 16 May 2018.

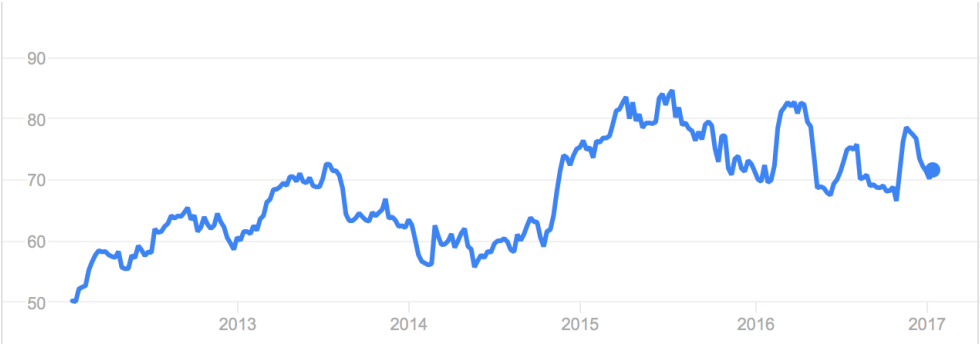

Figure 1: Stock market value of Target Corp.

In practice, the distribution of real reputational costs has a long-term effect. Some organization will suffer no significant long-term reputation damage, while other companies will go bankrupt because of the disclosure of the data breach.[61] The former group are likely to consist of organizations with a stable customer base that are able to exploit lock-in strategies and are too big to fail. A data breach does not reduce the likelihood that consumers buy the product or services of these organizations. The latter group has a small customer base and/or offers products with trust as a core selling point.[62] Nevertheless, the *perceived* value of reputation damage is more important than its objective value. As a security officer pointed out, "fear of reputation damage … drives organizations to take steps to at least evaluate, if not correct and enhance security mechanisms".[63] Alternatively, consider the following blog post: "Our head of IT Security (of a major telecom) told us once, 'we have one key metric: Don't show up in the Wall Street Journal for a security breach.'"[64]

A third issue is liability. The general logic is that when a data breach becomes public, the opportunity arises for the public to sue organizations. Therefore, notifying data breaches raises the likelihood of liability costs. Romanosky finds that when consumers suffer financial harm, the risk of litigation increases with a factor of 3.5.[65] However, two drivers mitigate this effect. First, a well-planned notification strategy for organizations can mitigate liability costs. Liability risks can be reduced when the organization is able to show that it took appropriate action in notification

---

[61] Robert Layton and Paul A. Watters, 'A methodology for estimating the tangible cost of data breaches' (2014) 19 Journal of Information Security and Applications 321 also indicate that firms can still grow, while writing-off some expenditures related to reputation damage.
[62] Compare for instance the 2017 Verizon data breach with the 2011 Diginotar data breach. The former did not encounter major issues while the latter went bankrupt.
[63] Op. cit. Mulligan (n 47) 14.
[64] See the following article on Bruce Schneier's blog: Bruce Schneier, 'Breach Notification Laws' (*Schneier on Security,* 21 January 2009) <https://www.schneier.com/blog/archives/2009/01/state_data_brea.html> accessed 16 May 2018.
[65] Op. cit. Romanosky, Hoffman and Acquisti (n 8) 76. This research is based on US data where the use of liability law is more common than in other jurisdictions.

and reduction of the risk (such as immediate disclosure itself). In the U.S., the likelihood of an organization being sued is six times lower when the organization offers free credit monitoring after the data breach.[66] Second, when a company intentionally conceals data breaches and they nevertheless become public, it can reasonably be expected that the likelihood and impact of claims will be higher. We summarize private costs and benefits in table 2 below.

Table 2: summary of private costs and benefits

Private benefits	**Marginal private benefits relative to a decreasing notification threshold**	**Private costs**	**Marginal private costs relative to a decreasing notification threshold**
Mitigation of impact and improvement of security	Decreasing	Administrative costs	Slight decrease
Reduction in reputation damage	Decreasing	Reputational damage	Decreasing
		Additional perceived reputation damage	Decreasing
		Liability costs	Decreasing

Private benefits and costs are strongly correlated with the magnitude of the data breach risk. Private benefits become higher when data breaches that have to be notified are more risky, while decreasing when breaches become less risky. With regard to private costs, we expect these administrative costs of disclosure to decrease slightly. This is related to the assumption that the administrative procedure to inform customers will take slightly more time when the breach is more significant because it can be expected that data subjects demand more information. We expect the other marginal private costs to decrease relative to a decreasing notification threshold. Concerning absolute numbers, private costs are (perceived as) high and certain, while private benefits are indirect and uncertain. Hence, we assume that (at least in the perception of the organization that has the notification duty) the private costs of data breach disclosure are higher than the private benefits. Ergo, there are few incentives for a private actor spontaneously to notify data breaches in the absence of the obligation.[67]

[66] Ibid 91.

[67] Surely, there are data breaches for which private benefits of disclosure exceed private costs. For instance, when there is a (perceived) high likelihood that a breach will be made public by a third party. In such a

5. The case for the DBNO

Section 3 observed that a data breach notification has social benefits, most notably bringing information to the market that serves as a right to know' and the information diffusion. Section 4 observed that data breach disclosure most likely imposes a net cost on private parties. There will not in most cases be spontaneous disclosure in the absence of the obligation. This section examines in 5.1 whether social surplus is likely to remain, even when net private costs are taken into account and argues that there is a case for regulation. Section 5.2 will distinguish the drivers important for sufficiently inducing data controllers to notify, despite their initial net private cost of doing so. Section 5.3 discusses the public cost of enforcing the DBNO.

5.1. Is there a case for the DBNO?

Most data breach disclosures impose a cost on data controllers. Up to the threshold, the social benefits outweigh the (net) private costs. Within this area, there is a case for regulation. The social optimal threshold for disclosure will lie a notch higher, because net private losses have to be added to the social costs. The data breaches below the threshold will have insufficient positive effects to compensate for the negative effects and generate a social loss. It becomes quite clear that this is important to give a direction for distinguishing and clarifying the threshold, which we will do in section 7.

5.2. Public cost of the DBNO

There are also public costs of the DBNO. The first is the adoption of the regulation as such. There are costs associated with the discussion and adoption of the regulation by the EU legislator. These are sunk costs and the regulator can also incur these costs when the regulation is not adopted. There are also costs involved in processing the notifications at the DPA. Furthermore, there are enforcement costs[68] and possible costs involved in offering a digital first aid kit, discussed in the next section.

---

situation the difference in reduced (perceived) reputation damage and the threat of liability claims may weigh against disclosure costs. There have been cases of spontaneous disclosure of data breaches in the past, although the 'spontaneity' of these disclosures is sometimes hard to disentangle from local legal obligations. For instance, in the Netherlands, there has been a local data breach notification law since January 1 2016 until the application of the GDPR. In addition, contractual obligations between parties could have triggered data breach disclosure in the past. Also, cases of spontaneous disclosure are hard to retrieve since there is obviously no obligation to notify a DPA in the absence of the law. To the best of our knowledge, there has been no further research conducted on the spontaneous disclosure of personal data breaches in the EU.

[68] Op. cit. Polinsky and Shavell (n 5); Sharon Oded, 'Inducing corporate compliance: A compound corporate liability regime' (2011) 31 International Review of Law and Economics 272, 273; George Stigler, 'The Optimum Enforcement of Laws' (1970) 78 Journal of Political Economy 526, 526.

Table 3: Public costs of a DBNO

Public costs (costs associated with the operation of the legal system)[69]	**Marginal public costs relative to a decreasing notification threshold**
Adoption costs	Sunk costs
Costs of DPA	Stable
Costs of enforcement	Stable for general enforcement, up to threshold violation specific enforcement
Costs of the digital first aid kit	Stable

When we add the public costs to the new social optimum, the socially optimal threshold becomes higher.

6. Will the EU DBNO sufficiently induce data controllers to notify?

Section 3 argued that disclosure is socially beneficial for a certain area of data breaches (up to the threshold). Section 4 concluded that, for the majority of those data breaches, there would be insufficient incentives for spontaneous disclosure by private parties. Section 5 argued that there is a case for regulation, because these social benefits are higher than private costs, provided that the benefits of regulation outweigh the public costs of regulation. The question this section aims to address is whether the European regulation will sufficiently induce data controllers to notify those data breaches for which disclosure is socially beneficial.

6.1. The administrative fine

The administrative fine is the main design parameter that induces data controllers to notify within Articles 33, 34 and 84(4) the DBNO; especially Article 84(4) GDPR gives DPAs this power.[70] In the case of non-compliance with the regulation, DPAs are granted the power to impose an administrative fine of €10,000,000 or 2% of the undertakings turnover, whichever is higher. .[71] The fine can be imposed when the data controller conceals a data breach or does not notify in due time. The administrative fine has several theoretical advantages. First, the fine has a multiplication effect. The fine has an effect once imposed, as well as the threat of the effect than can be executed multiple times once data controllers comply. Thus, when the sanction is set at a

[69] Steven Shavell, 'The Level of Litigation: Private Versus Social Optimality of Suit and of Settlement' (1999) 19 International Review of Law and Economics 99, 100: "To amplify, the private cost of a suit is less than the social cost of a suit, for that includes the injurer's costs as well as the public costs (those costs associated with the operation of the judicial system)."
[70] Op. cit. Nieuwesteeg (n 24) 80. The majority of the DBNOs in the world apply penalties in order to deter non-compliance.
[71] GDPR, Art. 83(4).

deterrent level that forces all data controllers to comply, the sanction itself is costless, because it does not have to be executed. In such a situation, only the threat suffices.[72] Moreover, even if the fine has to be imposed, the fine itself is considered a socially costless transfer of money (contrary to other threats such as imprisonment).[73] Last, higher sanctions allow for lower levels of enforcement to remain an identical level of deterrence. The high sanctions in Article 84(4) GDPR consequently could save enforcement costs.

However, the high fine in Article 84(4) GDPR also has several disadvantages. For small data controllers, the maximum de facto fine will be lower because a high fine will go beyond their solvency.[74] Next, high sanctions can lead to over- and under- deterrence when the perception of the likelihood of detection differs from the actual likelihood of detection.[75] This phenomenon occurs especially when there is a low likelihood of detection. To be specific, data controllers could be incentivized to notify data breaches that are subject to mandatory notification (because they do not result in a risk for data subjects) just because they want to be 'on the safe side'. This assumes that the data controllers do not have exact information about the two thresholds. This is reasonable to expect, because currently the thresholds are not defined any further than the qualification of 'risk' or 'high risk' to the rights and freedoms of data subjects. In a situation of over-deterrence, data controllers will disclose data breaches for which disclosure is not socially beneficial and this will result in a social welfare loss. Furthermore, a high administrative fine can incentivize data controllers not to detect data breaches.[76] Closely connected, people show risk-seeking behaviour when facing losses. This undermines the deterrent effect of high fines.[77] A last disadvantage of the (high) administrative fine is that it will punish the organization itself (and thus the shareholders and customers) and not the people responsible for concealing the data breach.[78]

---

[72] See Giuseppe Dari-Mattiacci and Gerrit de Geest, 'Carrots, sticks, and the multiplication effect' (2010) 26 Journal of Law, Economics, and Organization 365, 365, compare the discussion in *supra* section 2.2 on perceived reputation damage.
[73] Op. cit. Polinsky and Shavell (n 5).
[74] Also, in practice, it is likely that most actual fines will be lower than the maximum, lowering their deterrent effect. Article 83(2) specifies several circumstances of the case that have to be taken into account for the actual determination of the fine, such as negligence and mitigation measures.
[75] Op. cit. Polinsky and Shavell (n 5).
[76] See also A. Mitchell Polinsky and Steven Shavell, 'Mandatory versus Voluntary Disclosure of Product Risks' (2006) Harvard Law School, John M. Olin Center for Law, Economics and Business Discussion Paper Series 564/2006, 4 <http://www.nber.org/papers/w12776> accessed 16 May 2018.
[77] See the seminal article of Daniel Kahneman and Amon Tversky, 'Prospect Theory: An Analysis of Decision under Risk' (1979) 47 Econometrica 263.
[78] See for a more extensive discussion op. cit. Polinsky and Shavell (n 5).

6.2. Enforcement of the fine

The administrative fine of the DBNO is high, but the expected value of the administrative fine is the magnitude of the fine multiplied by the likelihood of detection. Hence, its deterrent effect largely depends on the ability of the DPA effectively to enforce at acceptable social cost.[79] What should be the level of deterrence? The level of deterrence should exceed the net private cost that data controllers incur when disclosing a data breach.[80] This private cost is not static but varies across data controllers and will also be different for each data breach. Section 4 concluded that private costs are (perceived as) high and certain, while private benefits are indirect and uncertain. Hence, there is a significant gap between private costs and benefits that should be closed by an appropriate deterrent effect of the DBNO in order to induce an organization to provide sufficient notification.

The appropriate level of deterrence can be accomplished through enforcing the regulation and by increasing the likelihood of detection. The GDPR does not give further instruction on how to enforce the obligation, apart from the statement that enforcement should be 'strong' according to Recital 7. This section will discuss several possibilities for enforcement of the EU DBNO.

General enforcement concerns auditing random organizations to investigate whether they comply with the DBNO. General enforcement is characterized by the fact that it does not depend on the number of individuals who actually commit harmful acts.[81] An example of the current Dutch DBNO that will be replaced by the EU DBNO illustrates that general enforcement will be costly.[82] Suppose the Dutch DPA wants to achieve a likelihood of detection of 10% and it will be able successfully to find a data breach in half of the cases where one has occurred.[83] Then it must audit 20% out of the total number of 132,000 organizations in the Netherlands.[84] No more than 20 organizations per year can be audited by one FTE.[85] Hence, to audit 20% one needs 1320 FTE. Given an average annual total cost for skilled personnel of €100,000, the regulatory costs of enforcement rise to €132,200,000 per annum. In 2017, the total capacity of the Dutch DPA in Netherlands is 72,5 FTE, that can only be partially deployed for enforcement.[86] Suppose that 25% of the Dutch DPAs total capacity (18,125 FTE) can be devoted to general enforcement of the

---

[79] See also op. cit. Dari-Mattiacci and De Geest (n 72) and Gary Becker, 'Crime and Punishment: An Economic Approach' (1968) 76 The Journal of Political Economy 169. According to the theory of deterrence, the strictness of the stick equals the magnitude of sanction stick multiplied by the probability of detection.
[80] See *supra* section 4.
[81] Op. cit. Oded (n 68) 273.
[82] Op. cit. Laube and Böhme (n 9) 37.
[83] We assume 50% likelihood of detection because data controllers can quite easily actively conceal data breaches by for instancing removing log files about the breach.
[84] According to the Dutch estimation when the DBNO was adopted.
[85] Assuming 10 days FTE work for an intensive auditing procedure.
[86] See <www.autoriteitpersoonsgegevens.nl> accessed 16 May 2018. The Dutch DPA also has other tasks.

DBNO. This results in an actual likelihood of detection of around 0,27%. In addition, general enforcement causes significant administrative costs for the organizations that are subject to an audit. Many of them have nothing to hide and have to devote time and money to the auditing procedure, which aggravates the social cost of general enforcement. Ergo, we believe that general enforcement is not a socially efficient instrument to increase the deterrent effect of the DBNO.[87]

Ex ante risk based auditing is a more efficient means of auditing. This approach starts with prioritizing sectors or organizations that are most likely to violate the obligation. In the US, for instance, healthcare and financial institutions have been subject to data breaches relatively more often than other sectors.[88] In addition, DPAs can prioritize their enforcement efforts on those sectors where the disclosure of data breaches is most likely to lead to the highest social welfare increase. Logically, ex ante risk based auditing reduces costs because the average likelihood of detection is likely to increase per audit. However, this should be weighed against the cost of ex ante efforts in determining the risk. When these costs are kept sufficiently low, for instance through diffusing information about risk assessments across the EU, risk based auditing is preferable to general enforcement. However, a labour intensive auditing procedure is likely to remain.

Violation specific enforcement entails that the DPA enforces violations of the EU DBNO that are discovered by third parties, such as ethical hackers, the media and data subjects affected by the data breach.[89] Verizon suggests that third parties discover 27% of the data breaches that reach the public. Unfortunately, this does not mean that of all data breaches, 27% will be discovered in this way. Hence, we cannot exclusively rely on the discoveries by third parties when only a small proportion of data breaches reaches the public. Suppose that 10% of the organizations experience a data breach. When 1% of the data breaches reaches the public, 0.27% will be discovered by third parties (and 0,73% will be disclosed by the organization itself). For violation specific enforcement, it is necessary that third parties have sufficient incentives to notify the DPA. Consequently, they must be fully compensated for their costs in notifying the DPA.[90] Ideally, they must solely notify the DPA, because the DPA needs to determine whether disclosure to data subjects is socially beneficial. Otherwise, inducing third parties to discover data breaches could contribute to notification fatigue. Similar to the stimulation of third party disclosure, the DPA could also encourage data breach notification by whistle-blowers by compensating them for their

---

[87] Op. cit. Laube and Böhme (n 9) 37.
[88] Based on the US Privacy Rights Clearinghouse data set that is for instance analysed by Benjamin Edwards, Steven Hofmeyr and Stephanie Forrest, 'Hype and Heavy Tails: A Closer Look at Data Breaches' (2016) 2 Journal of Cybersecurity 3, 4.
[89] Op. cit. Verizon (n 37) 3. When the risk of third party disclosure is very high, it will have the same effect as intense enforcement, but we assume that this is not the case; White hackers penetrate security systems in good faith in order to check security.
[90] Gerrit de Geest and Giuseppe Dari-Mattiacci, 'The Rise of Carrots and the Decline of Sticks' (2013) 80 University of Chicago Law Review 341, 363.

private losses. The fact that violation specific enforcement capitalizes upon the efforts of third parties or whistle-blowers, leads to the conclusion that it could be a more socially beneficial type of enforcement than ex ante enforcement, because the DPA does not have to engage enforcement activities with an uncertain outcome. On the downside, the level of deterrence will fully depend on the capacity of those parties to discover data breaches.

6.3. The digital first aid kit

Section 4 demonstrated that spontaneous disclosure in the absence of the obligation is unlikely. In addition, a mere data breach notification obligation without additional incentive schemes for compliance will not yield sufficient spontaneous disclosure. The previous section discussed the deterrent effect of the threat in the EU DBNO. It is likely that, although the lawmaker is fully informed, they are not able to set deterrence at such a level that it will induce data controllers to notify at a socially acceptable cost. This is related to the fact that the ex-ante enforcement of administrative sanctions in the DBNO is costly and that ex post enforcement depends significantly on third parties. Theoretical and empirical evidence[91] supports this statement, although there is limited attention in the literature to the effect of the unprecedented high administrative fines of the EU DBNO in the GDPR. The question arises of whether there are other complementary options available that can further induce data controllers to comply with the DBNO at reasonable social cost. In this and the next section, we will focus on those options that do not involve a significant alteration of the GDPR. Instead, we focus on more feasible incentive schemes, which can be implemented within the scope of the GDPR.[92]

When it is expected that most data controllers will conceal data breaches or will refrain from detecting them, rewarding compliance (offering 'carrots') may have lower costs than sanctioning and detecting violators (using 'sticks').[93] The single 'carrot' that we will discuss is the possibility for the DPA to provide the organization with specific tailored information that can reduce the

---

[91] Op. cit. Laube and Böhme (n 9); Op. cit. Nieuwesteeg (n 24) 110. Also there is anecdotal evidence that there is under-compliance in the case of the Dutch DBNO, see for instance: Rob de Lange, 'Bedrijven negeren Wet meldplicht datalekken' (*Het Financieel Dagblad,* 1 February 2017) <https://fd.nl/economie-politiek/1185463/veel-bedrijven-negeren-wet-meldplicht-datalekken> accessed 16 May 2018.

[92] For instance, criminal penalties are not provided for in the GDPR. However, the GDPR allows certain administrative fines to be fined as a criminal fine because of the legal system of some of the Member States and sometimes the Member States are free to choose the type of penalties when they have not being harmonized (Recital 151 and 152 GDPR). This is also related to the competence of the EU. See for example Paul Graig and Grainne de Burca, *EU Law: Text, Cases and Materials* (6th edn, Oxford University Press 2015). Criminal penalties have two advantages. First, they hit certain natural persons directly. Second, a criminal penalty is insensitive for the financial situation of an individual (the limited individual wealth issue of administrative sanctions is not of concern) when the criminal penalty is non-monetary (op. cit. Polinsky and Shavell (n 5).

[93] Donald Wittman, 'Liability for harm or restitution of benefit?' (1984) 13 Journal of Legal Studies 57 has analysed the role of administrative costs. He argued that if most organizations do not comply with the law, which is the expected outcome of the EU DBNO, rewarding compliers is cheaper than punishing violators.

impact of the data breach and reduce reputation damage; the 'digital first aid kit'.[94] In other words, if data controllers know that the DPA has essential information that will assist them in being resilient concerning the data breach, they will have additional incentives to disclose. This section discusses its opportunities, drawbacks and pre-requisites.

Opportunities. Rewarding compliance works best in situations when organizations have different effort costs in complying.[95] This is the case in complying with a DBNO. The disclosure of more risky data breaches will have a higher cost than the disclosure of less risky data breaches. The advantage of the digital first aid kit is that it can offer greater rewards for more risky data breaches in the sense that for more risky data breaches the value of useful assistance is also higher. Furthermore, the digital first aid kit benefits social welfare because it propels the diffusion of information in cyber security. For this, it is necessary that the costs of the stimulation of information diffusion remain lower than its benefits. This can be achieved through cooperation between national DPAs and automation of the first aid kit regarding its internal decision making process, about which information to give to which data controllers

Drawbacks. Rewarding compliance has more transaction costs than penalties, because the former has to be carried out each time the data controller complies, and the latter only has to be executed when the data controller does not comply with the regulation.[96] However, this effect is partly mitigated by the fact that high enforcement costs are likely to prohibit the lawmaker from setting deterrence at such a level that it will induce data controllers to notify at a socially acceptable cost. To put it simply, there will still be many violators because the deterrent level cannot be set sufficiently high. However, the digital first aid kit has additional social benefits that justify some cost in their execution. A second drawback is that rewarding compliance can have distortive effects on the equal distribution of goods when not applied uniformly.[97] Indeed, some organizations will experience more benefits than others will and this is something to be taken into consideration within the execution of the rewarding scheme. In this context, a third drawback is that a compliance rewarding scheme can create moral hazard, especially when the digital first aid kit would provide valuable information on cyber security that data controllers would otherwise have to pay for. The specific design should therefore take the risk of moral hazard into account.

---

[94] Another possible compliance rewarding scheme is the reduction of liability for data breaches when a data breach is notified in due time. However, liability is largely regulated by private law within the Member States and therefore does not fall within the scope of the GDPR. In addition, the DPA could offer a monetary compensation for the administrative costs in notifying a data breach. However, this can be costly and can have perverse and distortive effects and therefore we will not discuss this option.
[95] Op. cit. De Geest and Dari-Mattiacci (n 90) 367.
[96] Op. cit. Dari-Mattiacci and De Geest (n 72) 365.
[97] Op. cit. Wittman (n 93) 68.

Pre-requisites. First, it is indispensable for the DPA to invest in becoming a hub and knowledge centre for diffusion of data breach information.[98] It is required that the DPA is able quickly to categorize the data breach and estimate whether the organization affected needs assistance and which information it is relevant to provide. National DPAs can benefit from the European Union's wide application of the GDPR.[99] This requires that the DPA can quickly make an estimation, based on the nature of the data breach and the mitigation measures, to assess which lessons learned from other data breaches in their database should be transferred to the organization making the data breach. An import aspect is the implementation of a continuous feedback loop that tests whether the information was in fact valuable for the organization. Advanced data analytics is necessary here. Second, in order to achieve the desirable network effects of information diffusion, the enforcement and investments in knowledge, related to the digital first aid kit, must be above average in the early stages of the application of the GDPR. The digital first aid kit solely functions when information about best practices and mitigation measures is already there. Hence, this information needs to be obtained first without the digital first aid kit. This necessitates excessive enforcement in the early stages of the GDPR in order to generate the necessary data breach notifications to propel the network effects.

6.4. The expressive function of the DBNO

Section 6.1 showed that enforcement based on penalties is costly. As security economists, Laube and Böhme conclude that after modelling mandatory data breach disclosure: "Security breach notification laws *without* security audits, regardless of the level of sanctions, cannot incentivize firms to report security breaches to authorities, given positive disclosure costs."[100] However, despite the lack of positive incentives to do so, data breaches are still notified in the Netherlands and the U.S. without enforcement.[101] The fact that organizations have disclosed data breaches despite clear incentives not to do so, can be attributed to the likelihood of detection through third party enforcement. However, it could also be attributed to the expressive function of the regulation, which is another scheme that affects the incentives of organizations. Through its expressive function, the regulation affects behaviour by internalizing social norms.[102] The basic premise is that data controllers can gain utility from the fact that they are compliant with the regulation.[103] Stimulating the expressive function is a socially cost-efficient way to persuade

---

[98] See *supra* section 4.1.
[99] Already stressed in the GDPR, Art. 60, 61 and 62.
[100] Op. cit. Laube and Böhme (n 9) 19.
[101] Op. cit. Nieuwesteeg (n 24) 69 and for instance: Pim van der Beek, 'Autoriteit registreert 700 meldingen datalekken; (*Computable*, 8 March 2016) <https://www.computable.nl/artikel/nieuws/security/5716753/250449/autoriteit-registreert-700-meldingen-datalekken.html> accessed 16 May 2018.
[102] Robert Cooter, 'Expressive law and economics' (1998) 27 Journal of Legal Studies 585; Robert Cooter, 'Do good laws make good citizens? An economic analysis of internalized norms'(2000) 86 Virginia Law Review 1577.
[103] Francesco Parisi, *The Language of Law and Economics* (Cambridge University Press 2013) 113.

private parties, since there are almost no variable social costs involved. The EU DBNO can have a strong expressive function, based on its two core societal goals.

Right to know of individuals. The expressive function of the EU DBNO on protecting the fundamental right to the protection of personal data is already present. It is embedded in the broader GDPR that aims to execute the fundamental rights to the protection of personal data.

Information diffusion and its contribution to cyber security. The EU DBNO can have an expressive function in the fact that data breach disclosure can help others and contribute to overall cyber security. Apart from the directly beneficial digital first aid kit, discussed in the previous paragraph, the DPA could share certain information and the best practices of cyber risk management pro-actively. For instance, the DPA could build (anonymized) metrics about data breaches.[104]

6.5. Summary

Table 4 below displays the various incentive schemes to induce data controllers to notify, and their public costs.

Table 4: Incentive schemes and their social costs

Social costs	Incentive scheme	Marginal social costs relative to a decreasing notification threshold
Almost no social costs	Threat of administrative fine of €10,000,000 or 2% of the undertakings turnover	Stable
	Expressive function of the regulation	Decreasing
Low social costs	Violation specific enforcement	Stable
Medium social costs but compensated by social benefits	Digital first aid kit	Decreasing

[104] Building metrics about cyber data is one of the key challenges in cyber security economics, see for instance Hadi Asghari, Michel van Eeten and Milton Mueller, 'Internet Measurements and Public Policy: Mind the Gap' (2013) paper presented at The sixth USENIX Workshop on Cyber Security Experimentation and Test, Washington, D.C., 12 Aug. 2013, <https://www.usenix.org/system/files/conference/cset13/cset13-asghari.pdf> accessed 16 May 2018.

Medium social costs (depends on intensity)	(Limited) Ex ante risk based auditing	Stable
High social costs	General enforcement	Stable

7. Which disclosure threshold design of the EU DBNO will contribute to social welfare?

Section 6 discussed whether the EU DBNO sufficiently induces data controllers to comply with the regulation. If we suppose that a smart mix of incentives can indeed sufficiently induce sufficient data controllers to comply with the regulation, then the disclosure threshold determines the social benefits (or when set wrongly, the social costs) of the EU DBNO.[105] This section discusses the disclosure threshold for DPAs and data subjects.

7.1. The disclosure threshold for notification to DPAs

The GDPR defines the threshold for notifying to the DPA as those data breaches that result in a 'risk to the rights and freedoms of natural persons'.[106] How should this threshold be interpreted? In addition, should there be a difference in notifying to the DPA and data subjects? To begin with the last question: the difference between threshold notification to the DPA and data subjects can be explained quite easily because the total social costs of the former are only a fraction of the costs of notification to the latter. The organization that notifies has limited costs in providing the DPA with the necessary information (compared with communicating to an often large group of data subjects) and the DPA has limited costs in processing the information.[107] Moreover, it can already provide the organization with its 'digital first aid kit', which generates social benefits. Social costs such as the administrative costs of the data subject and notification fatigue do not manifest themselves when only the DPA has to be notified. Hence, the threshold for notification to the DPA should be low, especially because the DPA itself might be better able to judge whether an additional notification to data subjects is necessary from a social welfare perspective.[108]

7.2. The disclosure threshold for notification to data subjects

In the case of notification to affected data subjects, the GDPR raises the threshold in Article 34 by adding that in this case the risk to the rights and freedoms of natural persons should be 'high'

[105] See *supra* section 2.
[106] GDPR, Art. 33.
[107] See *supra* section 5.2.
[108] And it has the power to do so ex GDPR, Art. 34(4).

(Article 34).[109] This incremental threshold can be explained,, because the social costs of notification to data subjects are much higher. First, data breach disclosure to data subjects in general results in a larger net private loss because of reputation damage, higher administrative costs of disclosure (compared to notifying solely to the DPA) and the potential liability costs.[110] Second, there are also significant social costs of data breach disclosure, such as the administrative costs of processing the notification by affected data subjects and notification fatigue.[111] On the other hand, notification to data subjects generates most of the 'right to know' and information diffusion social benefits.[112] The DPA should specialize in estimating in which situations costs outweigh benefits and give clear guidelines and examples of when the data controller should notify and when not. A higher threshold for notification to data subjects in combination with a relatively low threshold for notification to DPAs is preferable. In a case where the data controller wrongly interprets that, it should not notify data subjects according to the high threshold, Article 34(4) allows the DPA to require that the organization notify data subjects anyway. This reduces the likelihood that data breaches are disclosed that are not socially beneficial and corrects this under-estimation.

7.3. Smart thresholds

Under the current regime, there are two actors that can decide whether to notify data breaches to the public: the data controller itself ex Article 34 GDPR and the Data Protection Authorities (DPAs) ex Article 34(4) GDPR. The analysis above describes the optimal disclosure threshold within the scope of the regulation for both actors. When we allow ourselves to think slightly beyond the current Articles 33 and 34 of the GDPR, other solutions emerge for a 'smarter' threshold.

There are strong arguments for an intensified role of the DPA in the notification procedure. This is related to the fact that DPAs can build up expertise in determining the threshold, being a repeat player, in contrast to individual data controllers who are unlikely to be involved more than once.[113] The approach followed in the GDPR to rely primarily on disclosure to the DPA, can therefore be understood precisely since the potentially averse consequences of notification (notification fatigue and reputational damage) will arise especially in case of notification to data subjects. One could even raise the question whether a notification to data subjects does have a benefit. Does a system of a notification to the DPA not suffice whereby the DPA, according to

---

[109] See *supra* section 2.
[110] See *supra* section 4.2.
[111] See *supra* section 3.3.
[112] Op. cit. De Hert and Papakonstantinou (n 13), 192: compared to earlier versions of the GDPR, the notification requirement for consumers is a 'notch' higher, as former versions did not include the requirement that the risk should be high.
[113] Marc Galanter, 'Why the "Haves" Come Out Ahead: Speculations on the Limits of Legal Change' (1974) 9 Law and Society 95, 97.

Article 34(4) GDPR, decides whether information to the public is necessary? In most cases it probably does. However, there may be situations of data breaches where a mere notification to the DPA may not suffice, for example, because potentially higher damage could result to data subjects if no immediate action is taken. The notification to the DPA could then slow down further action, especially because it is not known whether the DPA will indeed inform the public. Therefore, although notification to the DPA has priority, for cases where the data breach could result in high risks, it is still important to impose a subsequent duty to notify data subjects as well.

A more intensified role for the DPA also complements the discussion on the 'digital first aid kit' in section 6.3. When DPAs develop expertise to assist data controllers on mitigating damage, it can reasonably be assumed that they also are in a better position to determine whether notification to data subjects increases social welfare. The question is thus which decision-making model should form the basis for the DPA to decide whether notifications that they have received from data controllers should also reach the public, given the social cost and benefits of such a notification. The following three areas of expertise are of relevance. The DPA should first be able to distinguish whether there is direct action needed by the data subjects. When direct action is needed, the data breach notification should be notified in any case, to the extent that the benefits of these actions exceed the administrative costs on the side of the data subject. Second, the DPA should be able to qualify the impact of the data breach on the rights and freedoms of data subjects, for instance, by breaking down data breaches in low, medium and high impact breaches. A third area of expertise concerns the estimation of notification fatigue and especially the level in which it becomes problematic. Concerning notification fatigue, it could be desirable to make the notification decision contingent upon the previous amounts of notifications to a data subject. Here the DPA can utilize the stream of academic literature from behavioural economics.

8. Concluding remarks

From May 25 2018 onwards, the European Union finally has a general data breach notification obligation (EU DBNO) as part of the General Data Protection Regulation. We conclude that most data controllers will not spontaneously disclose in the absence of a regulation. The simple reason is that the private costs of notification are higher than the social benefits. This indeed necessitates regulation from a social welfare perspective, provided only data breaches that surpass a threshold are disclosed to the public. We conclude that the two main challenges of the EU are to induce data controllers to notify and to set the notification threshold at a socially acceptable level. Regarding the former, we argue that solely relying on deterrence will potentially be very costly or result in a limited likelihood of detection, even if ex ante risk-based auditing or ex post violation specific enforcement are taken into account. It is hard to predict the effects of the high administrative fine provided for in the GDPR. It could either lead to under-deterrence, given the low probability of detection, or to over-deterrence leading to too many notifications and thus to notification fatigue. The precise direction may depend upon the risk attitude of the data

controllers and on their (subjective) assessment of the probability of detection. However, both risks point to the limitations of a deterrence approach.

We encourage the DPA to study rewarding compliance and the expressive function of the regulation, as alternative incentive schemes. Especially, the digital first aid kit can be a promising additional incentive for data controllers to comply, provided that DPAs develop themselves as a centre of expertise in mitigating data breaches. Regarding the latter (the optimal level of the threshold) our analysis clarified that data breach disclosure can be a costly exercise from a social welfare perspective. Notification fatigue and the administrative costs of affected data subjects in particular negate social benefits when large amounts of insignificant data breaches are being disclosed to the public. Hence, the threshold for notifying to data subjects needs to be fairly high and clear-cut. The threshold for notifying the DPA can be much lower.

Unfortunately, there is little empirical research in this area. There are some data on data breaches, but for example, little is known about the effects of other obligations to disclose breaches of personal data. The entire EU DBNO is, therefore, largely based on assumptions about how data controllers will react to the DBNO, given the particular sanction regime. We have already indicated that, even theoretically, it is difficult to predict the effects of the regime, as it strongly depends on specific assumptions. Those may be crucial to determine the effectiveness of the DBNO. Once the DBNO has been put in place (in May 2018), it will be interesting to examine its effects based on empirical studies. Thus far, the predictions as to the effects of the DBNO remain largely based on theory.

The EU DBNO can be a welfare-enhancing piece of legislation, provided that it is wisely enforced and executed by national DPAs. Naturally, the social effects of the DBNO depend upon the actions taken by the DPAs after they have received the information on data breaches. Ultimately, if notifications merely end up in a digital drawer at the DPA and no further action is taken to promote data security, then obviously the entire DBNO would become an extremely costly exercise, without any social benefits as far as improving cyber security is concerned. This points to the crucial role to be played by the national DPAs in making the EU DBNO a success.

Acknowledgment
We are grateful to an anonymous reviewer, to the members of the European Doctorate in Law and Economics (EDLE) community, to the participants in the Annual Conference of the European Association of Law and Economics (EALE) in London, and to Gabriel Doménech Pascual for useful comments on an earlier version of this paper and to Nathalie Ahsmann and Teun Steenbergen for their editorial support.