THE CENTRE FOR internet & society

Breach Notifications: A step towards cyber security for consumers and citizens

By **AMELIA ANDERSDOTTER**

Designed by **Saumyaa Naidu**

Table of Contents

Through the Digital India project, the Indian government is seeking to establish India as a digital nation at the forefront. Increasingly, this means having good cyber-security policies in place and enabling a prosperous business environment for companies that implement sound cyber-security policies. This paper will look at one such policy, which enables investments in cyber-security for IT products and services through giving consumers a way to hold business owners and public authorities to account when their security fails.

1. Background

Electronic data processing has awarded societies with lots of opportunities for improvements that would not have been possible without them. Low market entrance barriers for new innovators have caused a flood of applications and automations that have the potential to improve citizens' and consumers' lives, as well as government operations. But while the increasing prevalence of electronic hardware and programmable software in many different parts of society and industry, combined with the intricate value chains of international communications networks, devices and equipment markets and software markets, have created a large number of opportunities for economic, social and public activity, they have also brought with them a number of specific problems pertaining to consumer rights.

As the value chains have grown longer and more complex, and trade is increasingly global, consumers suffer from an information deficit with respect to service providers and product retailers.

The entirety of the value chain may no longer be obvious to the consumer, as electronic network operators, internet exchanges, app developers, financial data management companies, advertisers, government identity providers or even ATM machine software providers all cooperate to provide a seamless consumer or citizen experience.

Concurrently with the development of more complex value chains, there has been a push for outsourcing of government functions to the private sector. Consequently, information <symmetries increase also in citizen interactions with the government. While electronic systems have been put to use for government functions all over the world for more than half a century, the provision and maintenance of these systems by private sector data processors (who effectively act as an intermediary between the citizen and the government) has an impact on the relationship between the citizen and the government which may not be obvious for the citizen. A security failure in either the government's software or in the private sector data processors' software (or hardware) may cause harm to the citizen, and the citizen has no way of tracing the harm to the software or hardware.

Importantly, product cycles in the electronic industries are short. This applies to both software and hardware. A regular office software suite may require security updates every week or at least every month. Apps are installed and de-installed on a daily basis. Office computers are replaced by companies and government authorities within three to five years, and mobile phones are replaced by consumers even more often. This calls for special attention to security measures, and especially careful evaluation of certification requirements.

Consider the mechanical auto-mobile industry, where after being certified and deployed on the market the vehicle may well operate as intended for several decades without the performance of the vehicle being significantly degraded. Even with extensive and time-consuming certification processes, the life-cycle of the product is longer than the certification-cycle. This is not the case of most software, and for some electronic apparatuses it is also not the case.

If the product cycle is likely to be shorter than the time it takes to certify the product, certification will not help establish consistent cyber-security levels. For this reason (among others) software certification programs like the Common Critera have been criticised[1] but a

practical example is the European Privacy Seal awarded to Microsoft in 2008.[2] The seal was restricted to specific versions of the Microsoft software, and Microsoft had to void the seal to make a security update only a short time after it was rewarded.

I will argue in the following that we need stronger consumer and citizen protection in the cyber-markets, and that enforcing stronger protection of consumers in these markets has the potential to enhance cyber-security where it matters the most. For this purpose, I will use the term “data subject” to refer to both consumers and citizens, and the word “data controller” to refer to the entity, either a private business or a government authority, which somehow collects, stores or processes data from the data subject in such a way that it is capable of being affected by a security breach. A security breach, in turn, means an event which causes data to be disclosed, or risk being disclosed, to parties not authorised to have access to the data.

In particular, I will make the case for obliging data controllers to inform data subjects about security breaches. We will call the information passed to data subjects a “breach notification”.

2. Breach Notifications - A History

2.1 The United States

An obligation to notify breaches is a measure aimed at establishing the right of data subjects to find out if data relating to themselves and preserver or collected by data controller has been wrongfully disclosed. The first law world-wide to be enacted with such an aim was a Californian bill passed in 2002.[3] The underlying idea of the legislature was that data subjects who were not made aware of when a data controller has failed in their security practises, also could not hold such a data controller to account. Since 2002, an addition 46 states have enacted breach notifications laws.[4]

There is no federal law for breach notifications in the United States (“US”). Additionally, the state legislations differ in scope.[5] While some federal states limit the notification requirement to specific data that are seen as especially sensitive for data subjects (such as name, address or financial data),[6] other states include a significantly wider range of data the loss of which requires notification (electronic mail identifiers, phone numbers, et cetera).[7] In some states, data controllers are required to inform a data subject even in the case of loss of data which, when it is combined with other data, may make it possible for an unauthorised agent to make inferences about a data subject’s social, financial or medical status.[8] In practise, this means that breaches of pseudonymous or anonymous data would need to be reported if they could be combined easily enough with other sets of data in a way which compromises data subject interests. The meaning of the words “pseudonymous” and “anonymous” may be considered interchange here, since it is demonstrated that it is very difficult to anonymise data in such a way that it could never be used for re-identification purposes. However, whether the data is pseudonymised or anonymised, it would be up to courts to decide how far the limits of the notification requirements extend.

Most (but not all) states provide exemptions from the obligation to notify a breach when the leaked data has been encrypted or otherwise rendered unintelligible to a third party prior to the breach.[9] Presumably, the reason for this caveat is that unintelligible or encrypted data could not be used by culprits to harm the data subject’s interests. All states allow for notifications not to be immediate, if immediate notification would prejudice an ongoing law enforcement investigation.[10] In some cases, notifications can also be withheld for reasons of national security.[11]

The notification is mostly required to be in written form, but in some states telephonic notices or publicising information in widely circulated medias suffices.[12] Enforcement of these laws is, in most states, the responsibility of the attorney general, but some states have

left their breach notification laws without any enforcement.[13] In a handful of states, data subjects have the ability to bring legal action against data controllers who fail to notify,[14] but in the majority of states the legislator has not foreseen enforcement actions by data subjects themselves.

2.2 European Union

Since the introduction of breach notification laws in the US, notifications have become a popular instrument for mitigating security concerns also in the European Union ("EU").

The first legislative instrument for breach notifications was introduced through the ePrivacy directive in 2009,[15] and included an obligation on electronic network providers to notify privacy incidents to designated competent authorities[16] in each member state.

The breach notification obligations of the ePrivacy directive have subsequently been followed by security breach notifications in the recently adopted network and information security directive (hereafter "NIS directive")[17] and privacy breach notifications in the recently adopted General Data Protection Regulation (hereafter "GDPR"),[18] as well as by privacy breach notifications in the directive for the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties (hereafter "new DP directive").[19]

The major difference between US approach to breach notifications and the EU approach, is that the latter relies much more on public authorities to act as a filter between the data controller and the data subject. Only through article 34, GDPR, do data subjects in the EU have a partial right to breach notifications if the breach causes a "high risk to their fundamental rights". Articles 4.3 and 4.4 of the ePrivacy directive and articles 14.3 and 16.3 of the NIS directive, on the other hand, provides only for reporting to the public authority, thereby making it more difficult for data subjects to access information about data controller misbehaviour.

In some member states, such as Sweden, strong freedom of information laws make it possible for data subjects to request information from public authorities about breach notifications in specific instances.[20] Since both the NIS directive and the ePrivacy directive provide for public authorities to propose a remedy that the notifier could undertake to enhance their security, it could be envisaged that they would oblige the data controller to notify the data subject directly. However, this is not an explicit alternative provided for by law, but a measure the competent authority would have to tacitly imply from the ePrivacy and NIS directive provisions. Specific laws at the member state level may, indeed, prohibit such disclosures.

3. The Economics of Breach Notifications

An underlying assumption of breach notification laws is that an informed data subject can make informed decisions with regards to what data controllers they choose to rely upon for storage of their personal data or provisioning of information society services.

Breach notification laws are not the only example of measures undertaken by legislators to make companies or public authorities disclose information to the public in order for the public to evaluate the performance of those companies and public authorities. Food labelling and product labelling are common regulatory strategies to enhance consumer freedom and choice. Freedom of information laws or open data initiatives help individuals evaluate their governments. Product safety requirements and market surveillance mechanisms assist both consumers and regulatory authorities in finding out when dangerous products have been placed on the market, or what the value chains for specific products are. Market surveillance mechanisms can for instance help in finding out where a particular good is from, where it was manufactured or assembled. Increasingly, governments around the world are cooperating

around best practises for the sharing of such information between themselves, and distribution of such information to retailers and consumers.[21]

It is generally assumed that getting relevant information to relevant groups on the market, helps these groups to make appropriate choices for their own safety and, to a lesser extent, the safety of others. Informed consumer choices leading to bad products becoming unpopular is frequently referred to as the "invisible hand". Since breach notification laws have already been in place in many jurisdictions for several, we can begin to appreciate the efficacy of breach notifications in this regard.

3.1 Country reports

3.1.1 The United States

Quantitative analyses on the effects of breach notifications on the US market have demonstrated a low, but consistent, tendency among consumers to sue companies from the financial and health sectors upon receiving breach notifications.[21] In other sectors, the effects of breach notifications are smaller and some have questioned whether the liability framework is adequate.[22] It is, for instance, difficult for consumers to demonstrate harm that would enable them to hold data controllers not only morally, but also financially, accountable after a breach.

3.1.2 The European Union

The EU Commission undertook at scoping exercise in the summer of 2016 aiming to establish the efficacy of the ePrivacy directive, including the breach notification provisions.[23] The inquiry states, as a baseline assumption, that breach notifications amassed with the regulatory authorities so far had not proven to be, in and of themselves, sufficient to provide an incentive for better security.[24]

Scandinavian telecommunications regulatory authorities contributed to the Commission that the focus on only notifying breaches of personal information was too limited, and that they would like for the obligation to be extended to security breaches that do not involve personal data.[25] The majority of member state government, public authority and commercial respondents, however, said that they felt the breach notification obligation in the ePrivacy directive did not need to be kept in the directive, in light of the breach notification requirements included in the GDPR.[26]

Since neither the NIS directive nor the GDPR have yet entered into effect in the EU, it cannot be said with certainty that the EU framework for data protection or consumer protection would help data subjects in the EU demonstrate harm in courts following a breach.

3.1.3 Sweden

A Swedish Report of Official Commission Inquiry on Privacy established in summer of 2016 that the breach notification requirement in Sweden was coupled with few means for the telecommunications regulatory authority to undertake punitive actions against data controllers in the electronic network sector who suffered the breach due to carelessness.[27] The Inquiry suggested that this was cause to question the efficacy of the scheme.

The Inquiry did not touch upon the effects of notifications on individual data subjects or on media reporting, since data subjects are normally not provided with the information notified in the breach notifications.

3.1.4 Germany

In Germany, the breach notifications called for by the ePrivacy directive are collected by data protection authorities, rather than the telecommunications regulatory authority. The ePrivacy

directive is, however, not the only place in German law where data subjects may be informed about the security problems.

In the federal regulation establishing the Bundesamt für Sicherheit in der Informationstechnik (BSI), data subject interests are safe-guarded by an active role of data protection authorities which extends to these authorities obliging data controllers to inform data subjects about specific security risks in federal communications systems.[28] Because data protection is dealt with as a constitutional or human rights issue under German law, the regulation does not specify any rights for data subjects to find out about security risks posed to them by private companies.

3.2 Incentives and compliance

For any measure imposed on the government on any industry, the cost of compliance in relation to the benefits of the measure should be considered. The digital environment has been beneficial for entrepreneurs and citizens largely because it promises very low market entry barriers. Mandatory security requirements may raise the market entry barriers and decrease competition or disallow innovators who would have otherwise gone on to do great things from doing just that.

Breach notifications have the advantage of being cheap for any market actor to undertake. Since the cost of transmitting information is low, even a small company or a start-up could afford doing so. This is in contrast with certification requirements or government-imposed technical standards, which may be difficult or expensive to use.

We may also identify two competing theories of incentives on market actors from the experiences in the US and in the EU. One is that notifying data subjects about data breaches will allow the data subjects to make informed decisions about when to trust a data controller, and which data controller should be trusted. In other worse, data controllers who do not adequately protect personal data will suffer from reputational harm and consumers will choose to get their services provided by another data controller.

The other theory is that public regulatory authorities can perform regulatory oversight, given sufficient data and technical skill, will be able to hold data controllers to account on behalf of the data subjects or on behalf of the government.

3.2.1 Reputational harm

The theory of reputational harm stands a lower chance of succeeding in sectors where data subjects have little influence over subcontractors. This is true, for instance, in the recent bank security breach allegedly suffered by a major Indian ATM Network.[29] It is not clear that banks will switch providers of ATM services, regardless of how much bad will they suffer from a security breach, and it is also not clear how a data subject would advocate for their bank to do so. If the security breach is in the wholesale software or hardware markets, rather than in the retail markets, the data subjects' ability to act decreases.

Additionally, if reputational harm is to be relied upon as the primary incentive for improvements, in many industries change will only come at a relatively modest page.[30] While consumers have been demonstrated to respond positively to breach disclosures[31] and negatively to mishandling of personal data,[32] it is not clear that consumers who find out about a data breach, even one where the data controller has acted negligently, will act to switch providers of services.

For instance, large breaches at popular social network LinkedIn in 2016[33] or at British telecommunications services provider TalkTalk in 2015[34] did not cause consumers to desert those providers. While in the case of LinkedIn we may suspect network effects to be the cause of consumers remaining on the platform in spite of the breach, this could not be the case for TalkTalk, which operates in a competitive market for telecommunications services. More surprisingly, the breaches do not even seem to have caused either data controller any

financial losses.[35] This means investors do not see bad security as a reason to withhold money from data controllers.

In the wake of an increasing number of high-profile data breaches (cf. Yahoo[36] and Ashley Madison[37]), data subjects do seem to demonstrate a long-term tendency of losing trust in online platforms. This has been established in one US government survey,[38] an international survey by CIGI/Ipsos,[39] as well as in a Swedish national survey.[40]

One risk is that reputational harm is not suffered directly by the data controller, but by the collective of all data controllers, as more and more breaches become known and reported.

3.2.2 Regulatory oversight

The idea of regulatory oversight is that regulatory authorities can act on behalf of some entity, which may be a data subject but may also be a government interest or competitors, to ensure that data controllers maintain an adequate level of cyber-security. This oversight relies on one primary mechanism: a public authority can normally fine a data controller which does not comply with its demand, or, in some cases, the public authority can demand that key employees working for the data controller be jailed if the data controller does not comply with regulatory authority demands.

In the US, the Federal Trade Commission regularly brings cases against data controllers who have been unable to uphold their privacy and security commitments with respect to consumers.[41] In the UK, the Information Commissioner's Office levied a £400'000 fine against TalkTalk following the 2015 data breach.[42] Here, the fine acts as an additional signal to investors that data breaches are taken seriously by the government, and establish that bad security does not mean business as usual.

In the Netherlands, the legislator boosted the data protection authority's abilities to levy fines against data controllers with bad security practises in 2015.[43] The GDPR will establish a maximum threshold for fines at 4\% of the annual turnover of the enterprise found guilty of a particularly bad security practise,[44] but the effects of such fines remain to be seen. The GDPR enters into effect only in 2018.[45]

These fines may function to encourage cyber-security investments in the private sector, but it is less clear whether they will encourage cyber-security investments in the public sector. While the GDPR establishes a responsibility for data processors - subcontractors to data controllers - to ensure that their information security is kept at a high level, many EU countries have specific laws for specific public sector bodies regarding their data collection and use. In Sweden, it has been specifically proposed that public authorities would fall outside the scope of economic sanctions.[46]

Under the German BSI regulation (see above) the BSI may recommend specific measures to be implemented by public sector data controllers to increase security.[47] These recommended measures need not be restricted to the handling of personal data, but may also concern how to avoid becoming part of a bot-net, or being affected by ransomware, or avoiding products shipped with default passwords. A default password is a password which is the same for every product in a specific category or batch, and these types of passwords are increasingly a problem in the internet of things or in consumer routers.[48]

A similar function is performed by the US National Institute for Standards and Technology (NIST).[49] NIST will issue recommendations, guidelines and standards, including in the field of cyber-security, encouraging government authorities and private sector bodies to implement certain security enhancing measures. NIST also researches new measures and methodologies in the field of cyber-security, such as the operation of secure e-mail.[50]

The BSI functions are more or less replicated in the EU NIS directive, so a wider range of EU public authorities in all the 28 member states may be expected to start issuing guidelines and suggestions for industry when the NIS directive enters into effect.

A notable feature of the functions described above, exempting the NIS directive, is that the regulatory authority does not have the authority to issue requirements or demands to the private sector, but only recommendations. In the NIS directive, the issuance of demands is limited to specific actors in critical sectors, such as electricity, water or gas. A more contentious point in the NIS directive is what the implications are of cloud services being covered by the directive. In the public sector, requirements are issued to assist public sector bodies in procurement.

4 Reflections

Notifying data subjects of data breaches may not in and of itself be sufficient to guarantee more cyber-security investments, but it is an important first step. Without accountability, it is difficult to explore what forms of liability must be imposed on which market actors in order to provide adequate incentives for cyber-security investments. Even breach notifications intended primarily for public authorities are justified by the realisation that without knowledge and data, the public authorities will not be able to suggest relevant measures to mitigate cyber-security concerns.

A relevant second step, then, is to ensure that consumers and citizens can effectively hold individual data controllers to account when there has been a breach. In the EU, it is foreseen that data protection laws will be helpful in this regard. Additional measures may, however, be necessary in the consumer rights field,[51] since data protection laws typically award the data controller with large contractual freedom.

Litigation in the consumer rights field is likely to address some of the deficiencies of data protection laws, through creating a clearer picture of what constitutes an unreasonable contract clause for an information society service. In the Indian context, with consumer protection law already being an established field, what is missing, then, is the development of a data protection framework, clarifying for data subjects what level of cyber-security they should reasonably expect in their interactions with companies and public authorities.

Footnotes

[1] Steven J. Murdoch, Mike Bond, Ross Anderson How Certification Systems Fail: Lessons from the Ware Report Computer Laboratory, University of Cambridge. IEEE Security & Privacy, volume 10, issue 6, pages 40–44, Nov–Dec 2012. [[*http://dx.doi.org/10.1109/MSP.2012.89*]]

[2] European Privacy Seal. [*https://www.european-privacy-seal.eu/EPS-en/Three-New-European-Privacy-Seals-Awarded*]

[3] Cal. Civ. Code §§ 1798.29 and 1798.80-84.

[4] National Conference of State Legislatures. Security Breach Notification Laws. [*http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx*]

[5] Steptoe & Johnson LLP, Comparison of US State and Federal Security Breach Notification Laws – Current through January 21, 2016. [*http://www.steptoe.com/assets/htmldocuments/SteptoeDataBreachNotificationChart.pdf*]

[6] /E.g./ Del. Code Ann. Tit. 6, §12B-101(4).

[7] /E.g./ N.C. Gen. Stat. §75-61(10).

[8] /E.g./ Ga. Code Ann. §10-1-911(6).

[9] For an example to the contrary, see e.g. Alaska.

[10] See above, footnote 5.

[11] /E.g./ Guam, Indiana, Maryland, Michigan, Mississippi and Ohio.

[12] See above, footnote 5.

[13] /E.g./ Georgia, Kentucky, Montana.

[14] /E.g./ Alaska, California, Hawaii, Illinois, Louisiana, Maryland, New Hampshire, North Carolina, South Carolina, Tennessee, Virginia, Washington.

[15] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) as amended by Directive 2009/136/EC of the European Parliament and of the Council. [[*http://eur-lex.europa.eu/eli/dir/2002/58/2009-12-19*]]

[16] Art 4.3 and Art 4.4 in Directive 2002/58/EC.

[17] Art. 14.3 and Art. 16.3, Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. [[*http://eur-lex.europa.eu/eli/dir/2016/1148/oj*]]

[18] Art. 33 and Art. 34, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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 (General Data Protection Regulation). [[*http://data.europa.eu/eli/reg/2016/679/oj*]]

[19] Art. 30 and 31, Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [[*http://data.europa.eu/eli/dir/2016/680/oj*]]

[20] Among the grounds that may be invoked by the Swedish Telecommunications Regulatory Authority to classify materials in breach notifications are commercial interests of the notifier, but the exception is applied narrowly and only to specific data such as the percentage of consumers affected, or exact area in square kilometers affected. Normally, the cause for the security incident is still listed, e.g. "/a module in a switch suffered an interface lock-up./"

[21] Sasha Romanosky, David Hofman, Alessandro Acquisti, Empirical Analysis of Data Breach Litigation, WEIS 2012: [*http://weis2012.econinfosec.org/papers/Romanosky_WEIS2012.pdf*]

[22] Rachel M Peters, So you've been notified, now what? – The problem with current data breach notification laws, Arizona Law Review. 2014, Vol. 56 Issue 4, p 1171-1202. [*http://www.arizonalawreview.org/pdf/56-4/56arizlrev1171.pdf*]

[23] European Commission, Public Consultation on the Evaluation and Review of the ePrivacy Directive [*https://ec.europa.eu/digital-single-market/en/news/public-consultation-evaluation-and-review-eprivacy-directive*]

[24] European Commission, Q. 21 of the public consultation on the Evaluation and Review of the ePrivacy Directive.

[25] European Commission, contributions of Communications Regulatory Authority, Finland and Swedish Post and Telecom Authority. [*https://ec.europa.eu/digital-single-market/en/news/contributions-received-public-bodies-public-consultation-evaluation-and-review-eprivacy*]

[26] See [*https://ec.europa.eu/digital-single-market/en/news/contributions-received-public-bodies-public-consultation-evaluation-and-review-eprivacy*]

[27] SOU 2016:41, pp. 620-621, Hur står det till med den personliga integriteten? – En kartläggning av Integritetskommittén. [*http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2016/06/sou-201641/*]

[28] Act to Strengthen the Security of Federal Information Technology of 14 August 2009, § 5(4). See [*https://www.bsi.bund.de/EN/TheBSI/Functions/functions_node.html*]

[29] Economic Times, 20 October 2016, 3.2 million debit cards compromised; SBI, HDFC Bank, ICICI, YES Bank and Axis worst hit. [*http://economictimes.indiatimes.com/industry/banking/finance/banking/3-2-million-debit-cards-compromised-sbi-hdfc-bank-icici-yes-bank-and-axis-worst-hit/articleshow/54945561.cms*]

[30] Jane K. Winn, Are Better Security Breach Notification Laws Possible, 24 Berkeley Tech. L.J. 1133 (2009). Available at: [*http://scholarship.law.berkeley.edu/btlj/vol24/iss3/6*]

[31] Deloitte, Deloitte Australian Privacy Index 2015: Transparency is opportunity. [*https://www2.deloitte.com/content/dam/Deloitte/au/Documents/risk/deloitte-au-risk-privacy-index-2015-090516.pdf*]

[32] Richard Wahlund, Daniel Dellham, David Åberg & Erik Lakomaa, Anseenderisker och dataskydd, in Risker och riskhantering i näringsliv och samhälle, Stockholm School of Economics Institute for Research, 2016.

[33] LinkedIn Official Blog, Protecting Our Members, [*https://blog.linkedin.com/2016/05/18/protecting-our-members*]

[34] The Guardian, 6 nov 2015, Nearly 157,000 had data breached in TalkTalk cyber-attack. [*https://www.theguardian.com/business/2015/nov/06/nearly-157000-had-data-breached-in-talktalk-cyber-attack*]

[35] For instance, while TalkTalk did lose market shares between 2015 and 2016 according to Ofcom Fast Stats: Internet Statistics ([*https://www.ofcom.org.uk/about-ofcom/latest/media/facts*] [accessed 08.11.2016]), they have in fact been losing market shares for a number of years, and there is nothing presently to indicate that the data breach would have contributed to speeding up that process. Cf. Ofcom, The Communications Market Report 2016, Fig 4.17, [*https://www.ofcom.org.uk/__data/assets/pdf_file/0024/26826/cmr_uk_2016.pdf*] ; Indeed, in the aftermath of the data breach, TalkTalks revenues continued increasing, by 1.8% in the period. Cf. The Guardian, 2 feb 2016, TalkTalk counts costs of cyber-attack. [*https://www.theguardian.com/business/2016/feb/02/talktalk-cyberattack-costs-customers-leave*] ; Similarly, LinkedIn:s 2nd quarter and 3rd quarter reports from 2016 do not indicate any lashback from the big data breach reported in May of the same year. See LinkedIn 2nd Quarter Report, 2 Aug 2016. [*https://press.linkedin.com/site-resources/news-releases/2016/linkedin-announces-second-quarter-2016-results*] and LinkedIn 3rd Quarter Report, 27 Oct 2016. [*https://press.linkedin.com/site-resources/news-releases/2016/linkedin-announces-third-quarter-2016-results*]

[36] InfoArmor, 28 sep 2016, InfoArmor: Yahoo Data Breach Investigation [*https://www.infoarmor.com/infoarmor-yahoo-data-breach-investigation/*]

[37] The Guardian, 28 feb 2016, Life after the Ashley Madison affair. [*https://www.theguardian.com/technology/2016/feb/28/what-happened-after-ashley-madison-was-hacked*]

[38] United States Department of Commerce, National Telecommunications and Information Administration, "Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities", 13 maj 2016. [*https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities*]

[39] 2016 CIGI-Ipsos Global Survey on Internet Security and Trust [*https://www.cigionline.org/internet-survey-2016*]

[40] Internetstiftelsen i samarbete med Insight Intelligence och SICS samt svenska näringslivsaktörer och Stockholms landsting, Delade meningar 2, mars 2016. [*https://www.iis.se/docs/Delade-Meningar-2016.pdf*]

[41] FTC, Privacy & Data Security Update (2015), January 2016. [*https://www.ftc.gov/reports/privacy-data-security-update-2015*]

[42] The Guardian, 5 Oct 2016, TalkTalk hit with record £400k fine over cyber-attack. [*https://www.theguardian.com/business/2016/oct/05/talktalk-hit-with-record-400k-fine-over-cyber-attack*]

[43] /Cf./ Autoriteit Persoonsgegevens, 28 December 2015, CBP krijgt boetebevoegdheid en wordt Autoriteit Persoonsgegevens. [*https://autoriteitpersoonsgegevens.nl/nl/nieuws/cbp-krijgt-boetebevoegdheid-en-wordt-autoriteit-persoonsgegevens*]

[44] Art. 83, GDPR.

[45] Art. 99, GDPR.

[46] SOU 2015:39, Myndighetsdatalag, proposal for 27 §.

[47] Act to Strengthen the Security of Federal Information Technology of 14 August 2009, § 3(1)(9).

[48] /See e.g./ [*https://www.routersecurity.org*]

[49] [*https://www.nist.gov/*]

[50] /Cf./ Domain Name Systems-Based Electronic Mail Security (NIST Special Publication 1800-6) [*https://nccoe.nist.gov/projects/building_blocks/secured_email*]

[51] Michiel Rhoen, Beyond consent: improving data protection through consumer protection law [*https://policyreview.info/articles/analysis/beyond-consent-improving-data-protection-through-consumer-protection-law*]