Stanford – Vienna
Transatlantic Technology Law Forum

A joint initiative of
Stanford Law School and the University of Vienna School of Law

TTLF Working Papers

No. 76

Corporate Governance and Data Protection Risk in the US and the EU

Elif Kiesow Cortez

2021

TTLF Working Papers

Editors: Siegfried Fina, Mark Lemley, and Roland Vogl

About the TTLF Working Papers

TTLF's Working Paper Series presents original research on technology, and business-related law and policy issues of the European Union and the US. The objective of TTLF's Working Paper Series is to share "work in progress". The authors of the papers are solely responsible for the content of their contributions and may use the citation standards of their home country. The TTLF Working Papers can be found at http://ttlf.stanford.edu. Please also visit this website to learn more about TTLF's mission and activities.

If you should have any questions regarding the TTLF's Working Paper Series, please contact Vienna Law Professor Siegfried Fina, Stanford Law Professor Mark Lemley or Stanford LST Executive Director Roland Vogl at the

Stanford-Vienna Transatlantic Technology Law Forum
http://ttlf.stanford.edu

Stanford Law School
Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610

University of Vienna School of Law
Department of Business Law
Schottenbastei 10-16
1010 Vienna, Austria

About the Author

Dr. Elif Kiesow Cortez is a senior lecturer and researcher in data protection and privacy regulation in the International and European Law Program at The Hague University of Applied Sciences (THUAS), Netherlands. Elif is currently the chair of Law and Technology and coordinates both the AI & Legal Technology Minor and the Cybersecurity Minor at THUAS. Before joining THUAS, Elif was a John M. Olin Fellow in Law and Economics at Harvard Law School. Elif's doctoral research at the Institute of Law and Economics, University of Hamburg, Germany, was funded by the German Research Association (DFG). During her doctoral studies, Elif was a visiting fellow at Harvard Business School and a visiting scholar at Berkeley School of Law. Elif holds undergraduate degrees in law and in economics and her research is focused on utilizing economic analysis of law to provide recommendations for solving cooperation problems between public and private actors in the domains of data protection and privacy. Since 2018, Elif is an advisory board member for the CIPP/E Exam Development Board of the IAPP. Elif has been a TTLF Fellow since 2020.

General Note about the Content

Suggested Citation

This TTLF Working Paper should be cited as:
Elif Kiesow Cortez, Corporate Governance and Data Protection Risk in the US and the EU, Stanford-Vienna TTLF Working Paper No. 76, http://ttlf.stanford.edu.

Copyright

Abstract

Data protection and privacy compliance risks are increasing in number and growing in complexity for all organizations and especially for business organizations. This article provides a bird's eye view of the available literature and professional reports on the contemporary and very salient issue of data protection risk for companies, also considering the first impacts of recently established privacy laws such as the General Data Protection Regulation in the EU and the California Consumer Protection Act in the US. As a result, corporations' data protection practices are now also attracting more interest from shareholders and other stakeholders. Recent shareholder class actions indicate that there are potential information asymmetries between shareholders and the management of corporations regarding the assessment of data protection and privacy compliance risks. This article relies on economic analysis to understand why companies are likely to underinvest in data protection practices, given a certain risk environment. The article further analyzes the problem of misperception of data protection risk as well as its potential drivers. More generally, this article contributes to the assessment of data protection laws in the US and in the EU, focusing on incentives to bring lawsuits against companies after major data breach events on both sides of the Atlantic.

Keywords: Data Protection Risk, Risk Assessment, Class Action Lawsuits, Agency Problems, Information Asymmetry, CCPA, GDPR

Content overview

1. Introduction

Data protection and privacy compliance risks are increasing in number and growing in complexity for business organizations worldwide. Enhanced remote working requirements due to the COVID-19 pandemic also contributed to the new data protection risk exposure. This article provides an overview of the available literature and professional reports on the very important and contemporary issue of data protection risk for companies, considering the legal requirements of the General Data Protection Regulation (GDPR) in the EU and the California Consumer Protection Act (CCPA) in the US. This article relies on economic analysis to understand why companies are likely to underinvest in data protection practices, given a certain risk environment.

GDPR and CCPA are two of the most influential examples of the recent regulatory attention given to data protection and privacy. Such regulatory developments and their implications also draw the attention of shareholders, as evidenced by a number of shareholder class actions connected to privacy law infringements. The prevalence of these cases may indicate information asymmetries exist between shareholders and the management of corporations regarding the assessment of data protection and privacy compliance risks.

Large corporations with dispersed ownership models often rely on the existence of sufficient incentives to exercise appropriate control over managerial actions, also taking into account the disciplining function played by capital markets.[1] However, agency problems can be pervasive and augment the challenge of overseeing managers. In this article it will be argued that cybersecurity risk management is a domain for which

[1] Fama, E.F., 1970. Efficient Capital Markets: A Review of Theory and Empirical Work. *The Journal of Finance*, 25(2), pp.383-417.

extraordinary difficulties exist for monitoring efforts by management. Distinctive mechanisms have evolved in different jurisdictions for ameliorating agency problems that arise due to the separation of ownership and control and the related information asymmetries between management and shareholders.[2] Also, the degree to which managers are afforded latitude to decide matters can differ between the US and certain civil law countries in Europe. Irrespective of differences across capitalist economies with regard to financial market peculiarities and organizational firm characteristics, it can be argued that underinvestment in privacy risk management is posing problems for corporations everywhere, and shareholders are taking notice of the deficiencies.

The present article aims at providing insights with regard to the effectiveness of selected prominent data protection laws in the EU and in the US, focusing on the neglected dynamics driven by mandatory data protection risk reporting requirements and the possibilities that they open for stakeholders to sue companies after major data breaches.

The article will first make the argument that cybersecurity risk management poses particular challenges for corporations due to amplified agency problems (Section 3). Next it will discuss privacy risk reporting in the US and the European contexts (Section 4). This is followed by remarks about the economic fallout for companies in the event of non-compliance with data protection laws (Section 5). Lastly, major US and European cases of (collective) complaints brought by affected parties against companies in the aftermath of significant data breaches will be presented and briefly discussed (Section 6).

[2] Coffee, J.C., 2001. The Rise of Dispersed Ownership: The Roles of Law and the State in the Separation of Ownership and Control. *Yale Law Journal*, 111(1), pp.1-82.

2. Information Asymmetry Shareholder vs. Management

A 2019 survey of institutional investors representing US$35 trillion in assets regarding the biggest threats to portfolio companies' strategic success in the next three to five years ranked data privacy and cybersecurity third among risks.[3] Companies with specific intrinsic characteristics that create particularly pronounced information asymmetries are particularly exposed to cybersecurity risk. When this exposure leads to the occurrence of large data breaches, these firms can end up facing costly litigation, as discussed in Section 6. This section will discuss these asymmetries related to the data protection domain from a corporate governance angle.

Corporate governance can be basically characterized at its core as a problem involving the manager of a corporation and multiple potential principals – the shareholders, creditors, employees, and other parties with whom the manager transacts on behalf of the firm. Boards and external auditors function as intermediaries or represent some of these constituencies (Becht et al. 2007). This understanding of corporate governance was prominently laid out by Jensen and Meckling (1976), who depict the corporation as an entity succinctly as "a nexus of contracting relationships." This seminal article also happens to be a foundational work of principal-agent theory, which is concerned with the implications of asymmetric information between partners to a contract, for example a contract between the principal and an agent. In line with this, the challenge facing corporate governance can be also described as a "common agency problem" that involves one agent, the manager, interacting with multiple potential principals, including shareholders and employees (Bernheim and Whinston 1986).

[3] Klemash, S.W., Smith, J.C., and Seets, C., 2020. What Companies are Disclosing About Cybersecurity Risk and Oversight. Harvard Law School Forum on Corporate Governance. 25 August. Available at: https://corpgov.law.harvard.edu/2020/08/25/what-companies-are-disclosing-about-cybersecurity-risk-and-oversight/

Corporate governance rules emerge out of contracting efforts between the different principals or constituencies and the management of the corporation. Unless otherwise stated, the present article will focus foremost on the relationship between management and shareholders and the distinctive challenges data protection concerns and practices add to this relationship.

An important issue in corporate governance is to comprehend what the likely outcome of the contracting efforts between agent and principal is going to be, and how in practice corporate governance can deviate from a theoretically formulated efficient contracting benchmark. This article aims at offering an initial discussion of how the realm of compliance with data protection can pose new challenges for corporations, which can interfere with the nature of some of the corporations' agency relationships.

The information asymmetry that characterizes the principal-agent relationship between shareholders and management can generate moral hazard, situations that encourage excessive risk-taking by shielding the risk taker from the full consequences of the action. Moral hazard can stem from hidden information or hidden action (Hermalin and Weisbach 2017). Hidden information occurs when the principal does not have the expertise to properly assess the agent's actions. Hidden action occurs when the principal cannot even observe the agent's actions. In both cases asymmetric information gives the agent room to act in ways that are not in line with the principal's expectations. Thus, when for example a bad outcome materializes (e.g. the firm is caught mishandling private data), then the principal (the shareholders) cannot refute a claim by the agent (the management of the firm) that it happened due to a random exogenous shock and not because of faulty behavior by the agent. It is plausible to expect that both types of moral

hazard problems (hidden information and hidden action) can occur to a significant degree with regard to corporations' data protection practices.

The literature on the economics of agency emphasizes how the extent and the ease with which the agent can conceal actions becomes very important for the agency relationship and the possibilities of employing contractual solutions. In this vein, Hermalin (2017, p. 76) observes:

> Although it is hard to dispute that a key driver of corporate governance problems is asymmetric information, knowing what is asymmetrically known and by whom is critical. Does the agent possess payoff relevant information unknown to the principal? Does he take an action that the principal cannot observe? Or perhaps he takes an action that the principal can observe, but which is difficult for her to verify. As this chapter has shown, the nature of the contractual solution can vary tremendously depending on these issues; as can the resulting predictions.

Managers can have many opportunities to conceal data-handling practices from external oversight. One reason is that some aspects of data handling involve IT-solutions that non-experts have difficulty understanding. One consequence of this exacerbated agency problem can be managers underinvesting in compliance with the data protection regulations (Park 2019).

Park (2019) argues that the threat stemming from data breach litigation could in principle attenuate the agency problem and the related misaligned incentives to invest in robust security measures. However, for such a litigation threat to have the desired effect of inducing managers to shore up precautionary investment, it has to happen in a context

where the plaintiff has a reasonable chance of winning. Park argues that in the US context, California courts' reluctance to grant Article III standing impaired this type of solution based on a mechanism of private enforcement. Likewise Chatterjee and Sokol (2021) point out that firms spend much less on data breach related compliance than on other traditional areas of compliance such as anti-bribery and audit fraud.

Anderson and Moore (2006) point out another relationship fraught with information asymmetries, namely the one between management and software providers. When buying software, firms cannot verify the claims that software vendors make about the security of their products and thus firms have no reason to trust those claims. The software market turns into a market for lemons because buying firms are unwilling to pay a premium for quality they cannot measure, and therefore only lower quality software remains available for sale. Buying firms lacking the information needed to assess a software have no reason to pay more for protection, and consequently vendors are disinclined to invest in it (Akerlof 1970; Anderson and Moore 2006). This also contributes to suboptimal preparedness against data breach risk.

In terms of the regulatory response to the problem of corporate agency problems due to information asymmetry and the effect on companies' privacy policies, there are indications of differences between regulators in the EU and the US in how they perceive the severity of the problem and which solutions they deem most appropriate. Indeed, the CCPA provides for a lighter and less demanding regulatory approach than the GDPR at the intra-firm operational and institutional level. For example, the GDPR requires firms to put in place a data protection officer (DPO) and to conduct data protection impact assessments (DPIAs). The European approach seems to indicate that regulators east of the Atlantic have doubts that firms are likely to decide by themselves to reorganize

internally to better accommodate privacy risk challenges. This might stem from a recognition of European regulators that the problem of information asymmetries within corporate structures is particularly accentuated for the case of privacy risk since effective monitoring of management efforts in this domain is especially difficult for the relevant stakeholders and principals.

3. Organizational Vulnerabilities and Privacy Risks

The following two sections will consider corporations' vulnerabilities to data leakage incidents, review ways to assess the magnitude of the risks, and discuss corporations' underinvestment in cybersecurity despite evidence of exposure. Additionally, evidence as to the risk of attack according to firm type in the United States will be reviewed and the underlying theoretical underpinnings discussed.

3.1. Corporations' Cybersecurity Vulnerabilities and Private Data Leakage

Organizations are vulnerable to private data leakages due to human-induced errors and misperception of risks. Addressing these vulnerabilities effectively is difficult and requires sustained commitment from management. However, this commitment might be insufficient, as Section 2 will describe. Phishing and ransomware are two common forms of cybercrime.

Phishing is a cybercrime in which multiple users receive bulk e-mails written as if sent by a legitimate organization (such as a bank or a commercial firm) in order to steal data.[4] Personal data collected in this manner is used for criminal offences such as identity theft or for duplicating credit cards. Similar schemes directed at companies can allow

[4] Kostopoulos, G.K., 2017. Cyberspace and Cybersecurity, 2nd Edition. Taylor & Francis: New York.

cybercriminals access to their data such as trade secrets or intellectual property when an employee clicks on a phishing link.[5] One cybersecurity approach focuses solely on raising awareness among insiders in the believe that if everyone with access to a company's systems are well-trained not to click on phishing links, the systems can be protected.[6]

Ransomware is malware that encrypts the data in the computer of the victim. Cybercriminals then ransom the data by offering the decryption key for cash. In 2017, the WannaCry ransomware affected many users globally, bringing the attention of the general public to this significant data protection risk.[7] The Global Risks Reports 2018 of the World Economic Forum notes that the NotPetya ransomware attack caused an estimated harm to businesses adding of $300 million worldwide.[8] Petya and NotPetya attacks affected many global firms such as Maersk, Merck, and DLA Piper among many others.[9]

The exploitation of judgment errors by customers and employees provides a strong indication that calculations of cybersecurity risk should include the human factor. A recent study by Leukfeldt that included 10,316 respondents shows that neither personal background nor financial status predict susceptibility to phishing attacks.[10] Indeed, research has yet to identify what factors make individuals more likely to fall for hacker

[5] SANS Institute, 2017. Threat Landscape Survey: Users on the Front Line, Whitepaper, available at: https://www.sans.org/reading-room/whitepapers/threats/2017-threat-landscape-survey-users-front-line-37910
[6] Garfinkel, S.L., 2012. The Cybersecurity Risk. Communications of the ACM, 55(6), pp.29-32.
[7] Palmer, D., 2018. Ransomware: Not dead, just getting a lot sneakier. ZDNet. 3 July. Available at: https://www.zdnet.com/article/ransomware-not-dead-just-getting-a-lot-sneakier/
[8] World Economic Forum, 2018. Global Risks Report, available at: http://reports.weforum.org/global-risks-2018/global-risks-landscape-2018/#landscape
[9] Hern, A, WannaCry, Petya, NotPetya: how ransomware hit the big time in 2017, 30 December 2017, The Guardian, available at: https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware
[10] Leukfeldt, E.R., 2014. Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization. Cyberpsychology, Behavior, and Social Networking, 17(8), pp.551-555.

traps, but it is clear that cybersecurity awareness is generally low. Bruijn and Janssen discuss the reasons for this as well as some reasons companies do not investment in cybersecurity such as limited visibility, the ambiguous impact of attacks, and the incentives of victims to hide that they experienced an attack.[11] In their 2009 paper Harknett and Stever call on government to shape cybersecurity practices in consultation with private businesses and the general public, especially citizens who are well-informed about cybersecurity threats and solutions, as the only effective approach.[12]

According to the Cisco Annual Cybersecurity Report, 49% of participating organizations reported that they experienced public scrutiny after a data breach became public. Yet such scrutiny has not made them cautious; most organizations ignore 44% of the security alerts they receive.[13] As Cisco's Chief Security Officer notes in the report, paying attention to such alerts could readily bear fruit in blocking cybercrime.[14] Nevertheless, research shows that companies that have a dominant market position are behaving as if they are not afraid to lose their customers in response to an attack.[15]

The most recent Cybersecurity Cultures in Organizations report by the European Union Agency for Cybersecurity (ENISA) reveals the economic costs of cyberattacks and

[11] de Bruijn, H. and Janssen, M., 2017. Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, *34*(1), pp.1-7.
[12] Harknett, R.J. and Stever, J.A., 2009. The cybersecurity triad: Government, private sector partners, and the engaged cybersecurity citizen. Journal of Homeland Security and Emergency Management, 6(1).
[13] Cisco 2017 Annual Cyber security Report, available at: https://www.cisco.com/c/m/en_au/products/security/offers/annual-cybersecurity-report-2017.html.
[14] Ibid.
[15] On the 'public good' approach to cybersecurity and its potential consequence being underinvestment in cybersecurity by companies see Coyne, C.J. and Leeson, P.T., 2005. Who's to Protect Cyberspace? Journal of Law, Economics & Policy, 1(2), pp.473-495. For more on economics of cybersecurity and a 'cybersecurity as a public good' approach see Mulligan, D.K. and Schneider, F.B., 2011. Doctrine for Cybersecurity. Daedalus, 140(4), pp.70-92. and Moore, T. and Anderson, R., 2012. Internet Security. In: Peitz, M. and J. Waldfogel (eds.) *The Oxford Handbook of the Digital Economy*, Oxford University Press: Oxford, pp.572-599. On the analysis of regulatory strategies see van den Berg, B., 2016. Coping with information underload. In: Hildebrandt, M. and B. van den Berg (eds.) Information, Freedom and Property, Routledge: Abingdon UK, pp.173-199.

breaches.[16] These include direct costs such as loss of intellectual property and indirect costs such as loss of reputation (and market share due to reputation loss).[17] Citing several professional sources,[18] the report documents that occurrence of phishing and ransomware attacks is increasing in frequency and that the average ransom demanded from firms is increasing.[19] The report also emphasizes that the pervasiveness of global value chains is exposing an increasing number of firms to cybersecurity vulnerabilities.[20] Likewise ENISA's threat landscape report for 2020 shows that phishing, ransomware, insider threat, identity theft, and information leakage were on the rise.[21] The report admonishes organizations to update their cyber-threat-intelligence schemes with more trainings via cyber-ranges and calls for Cybersecurity R&D to focus on research initiatives on high-risk points of vulnerability.[22]

3.2. Quantification of Data Protection Risk and Underinvestment in Cybersecurity

Ralston, Graham, and Hieb focus on analyzing cybersecurity threats and risks for supervisory control and data acquisition and distributed control systems.[23] The paper states that protecting critical US infrastructure from cyber-attack and performing risk assessments in this regard became priority concerns for the Department of Homeland Security.[24] Increased connectivity and the technological developments also increased

[16] ENISA Cybersecurity Cultures in Organizations report, available at: https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations
[17] ibid
[18] 2017 – IBM – X-Force Threat Intelligence Index, available via https://www.ibm.com/security/data-breach/threat-intelligence, 2017 – Symantec – Internet Security Threat Report, 2016 – Verizon – Data Breach Investigations Report
[19] ENISA Cybersecurity Cultures in Organizations report, available at: https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations
[20] ENISA Cybersecurity Cultures in Organizations report, available at: https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations
[21] ENISA Threat Landscape Report 2020, available at https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends.
[22] Ibid.
[23] Ralston, P.A., Graham, J.H. and Hieb, J.L., 2007. Cyber security risk assessment for SCADA and DCS networks. *ISA transactions*, *46*(4), pp.583-594.
[24] Ibid.

the vulnerabilities of supervisory control and data acquisition systems, which were previously seen as isolated systems that are not subject to the same network threats as companies.[25] Quantifying the data protection risk could be more accurate if more data were available on the attacks and the consequences of these cyberattacks. However companies are not willing to share this information publicly for reasons such as damage to their reputation[26] or revealing vulnerabilities of their systems.[27]

Information on the probability and frequency of cyberattacks could help the companies better prioritize their investments in cybersecurity by allowing them to make risk calculations.[28] In their paper, Kaplan and Garrick differentiate an 'absolute risk', denoting a clear risk for people with full information, from a 'perceived risk', denoting an incorrectly assessed risk due to lack of information.[29] They explain that risk should not be perceived as "probability times consequences" because this would have the impact of grouping high probability attacks with low harm (consequences) and low probability attacks that would cause high harm.[30] The authors propose companies should approach risk as a whole, including all possible (probable) attacks.[31]

[25] Ibid.
[26] On how investors react to information security breaches of companies, see Gordon, L.A., Loeb, M.P. and Zhou, L., 2011. The impact of information security breaches: Has there been a downward shift in costs?. *Journal of Computer Security*, *19*(1), pp.33-56.
[27] On the risk of creating a road-map for future cybercriminals by disclosing vulnerabilities, see Ferraro, M.F., 2013. Groundbreaking or Broken; An Analysis of SEC Cybersecurity Disclosure Guidance, Its Effectiveness, and Implications. Alb. L. Rev., 77, pp.297-347.
[28] Kaplan, S. and Garrick, B.J., 1981. On the quantitative definition of risk. *Risk analysis*, *1*(1), pp.11-27.
[29] Ibid, p.12. The authors do not include the definition of the absolute risk and perceived risk but they differentiate by referring to a hypothetical scenario. In this scenario, they imagine a person puts a rattlesnake in another person's mailbox. They explain that if the mailbox owner were asked whether it would be taking a risk for him to put his hand into his mailbox, he would say 'no'. However, this response would only reflect the perceived risk as the mailbox owner lacks the information regarding the placement of the snake, not the absolute risk.
[30] Ibid.
[31] Ibid.

Research has analyzed perceived risk from a cognitive perspective, reporting that who informs the public about the risk and what kind of signal the public receives, i.e. whether the information is coming from a high-quality source, can affect the public's perception of risk.[32] Kasperson et al. provide a model explaining misperception of risk among the general public that can also be used to shed light on how stakeholders of companies might misperceive the risk of cyberattacks.[33] The model delineates four channels that contribute to individuals' misconception of risk: (1) *heuristics and value*: individuals introduce biases when deciphering information; (2) *social group relationships*: the interests of a social group affects risk perception; (3) *signal value*: newer risks with consequences that are not well amplify the perceived risk; and (4) *stigmatization*: individuals avoid environments associated with risk.[34]

Companies may be the victim of cyberattacks without even knowing it, as phishing attacks only come to light if the attacker chooses to inform the company of their illegitimate access to companies' systems. Therefore perceived risk may be far lower than absolute risk in this area. Likewise the economic impact of the cybersecurity breaches is not easy to calculate, which can also increase underestimation of the consequences of a cyberattack. This suggests that investment in cybersecurity awareness at the governmental, business, and citizen level[35] will contribute to ameliorating the lack of information that causes misperceptions of risk. Companies' increased cybersecurity awareness would be expected to focus their attention on their

[32] Kasperson, R.E., Renn, O., Slovic, P., Brown, H.S., Emel, J., Goble, R., Kasperson, J.X. and Ratick, S., 1988. The social amplification of risk: A conceptual framework. *Risk analysis*, *8*(2), pp.177-187
[33] For a recent study analyzing whether the news media amplifies the data protection risk see Reijmer, T. and Spruit, M.R., 2014. Cybersecurity in the news: A grounded theory approach to better understand its emerging prominence. Technical Report Series, (UU-CS-2014-006).
[34] Ibid, pp. 185-186.
[35] de Bruijn, H. and Janssen, M., 2017. Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, *34*(1), pp.1-7.

vulnerabilities and as a result, would lower the probability of harm caused by cyberattacks.

In cybersecurity research, cyber threats are typically analyzed together with attack vectors. Attack vectors are defined in the ENISA report as "a means by which a threat agent can abuse weaknesses or vulnerabilities on assets (including human) to achieve a specific outcome."[36] The report categorizes the attack vectors as follows: attacking the human element (through tactics such as phishing, customer support scams, and social media information gathering), web- and browser-based attacks (such as malvertising, SQL injection, and drive-by downloads), internet exposed attacks (when internet-exposed services are used to deliver malware or perform ransom attacks), exploitation of vulnerabilities (such as the WannaCry attack, which used previously leaked National Security Agency information to exploit a Microsoft Windows SMB vulnerability), and supply-chain attacks (such as the NotPetya malware which exploited a compromise of the systems of the legitimate accounting software M.E.Doc to attack users of the software).[37]

Confronted with cyber threats, companies are likely to underinvest in security measures. Given their basic profit motive, companies avoid paying for things they consider not essential, such as investment in cybersecurity. If many companies behave in this manner, this only increases the perception that cyberattacks are rare. Indeed, research indicates that group decisions and group behavior can lead to flawed risk assessment.[38]

[36] ENISA Threat Lanscape Report 2020
[37] ENISA Threat Lanscape Report 2017, pp.100-104.
[38] Kasperson, R.E., Renn, O., Slovic, P., Brown, H.S., Emel, J., Goble, R., Kasperson, J.X. and Ratick, S., 1988. The social amplification of risk: A conceptual framework. *Risk analysis*, *8*(2), pp.177-187

Kamya et al. provide information as to what types of firms are likely to experience data breach attacks based on a study of such attacks on U.S. firms in the period 2005 to 2017 collected by the Privacy Rights Clearinghouse.[39] For methodological reasons the data includes only attacks involving the breach of a firm's customer data are included, since the State Security Breach Notification Laws require such reports. Findings indicate that 30% of attacks occurred in the service industry, 27% in the financial sector, 18% in manufacturing industries, and 15% in wholesale and retail trade.

From a theoretical point of view, it is not clear what types of firms hackers are likely to target. Hackers are expected to attack firms where benefits surpass costs. On the one hand, more visible, larger firms might provide more personal customer data that can be misused and exploited for greater gain. On the other hand, smaller firms might be more vulnerable because their IT security systems are likely to be less sophisticated. Kamya et al.'s empirical model shows that larger firms are more likely to suffer attacks. In addition to sheer size, aspects connected to a firm's visibility increase risk: being part of the *Fortune* 500 list, being financially less constrained, being more highly valued, and possessing more intangible assets.

Kamya et al. find firms that face *less* competition in their respective market segment are more likely to experience an attack. They measure market competitiveness using the Herfindahl index as a measurement of the "uniqueness" of the firm's product, assessed using the ratio of selling expense to sales. An implication of this result could be that firms that "feel safer," in the sense that they do not fear losing market share to a competitor after an attack becomes public, might be investing less in securing their IT systems

[39] Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., and Stulz, R. M., 2018. What is the Impact of Successful Cyberattacks on Target Firms? NBER Working Paper No. 24409.

against attacks. These firms could be betting on the fact that a publicized cyberattack would cause only limited losses in revenue.

Kamya et al.'s regression results suggest that firms can be proactive when it comes to reducing data protection risk. The authors code a variable that captures if a firm possesses a "risk committee" on its board, information they obtain from BoardEx. A "risk committee" is defined as a board committee handling risk, which may go under names such as 'Risk Management Committee', 'Audit and Risk Committee', or 'Enterprise Risk Management Committee'. Controlling for the total number of board committees a firm possesses, the regression results show risk committees lower risk of a cyberattack. This may suggest that having an organization structure attentive to risk also increases firm awareness of cybersecurity risk, leading to implementation of effective cybersecurity measures.

3.3. Boards' Reported Cybersecurity Preparedness

Cheng and Groysberg (2017) and Cheng et al. (2021) discuss results of surveys they conducted that also covered the issue of cybersecurity awareness and preparedness among boards of corporations.[40] One of the reported findings is that one source of cybersecurity vulnerabilities for corporations is that boards do not have appropriate processes in place or sufficient (access to) expertise to identify, assess, and handle cyberthreats.

[40] Cheng, J. Y.-J., and Groysberg, B., 2017. Why Boards Aren't Dealing with Cyberthreats. *Harvard Business Review* (digital article). February 22. Available at: https://hbr.org/2017/02/why-boards-arent-dealing-with-cyberthreats; Cheng, J. Y.-J., Groysberg, B., Healy, P. and Vijayaraghavan, R., 2021. Directors' Perceptions of Board Effectiveness and Internal Operations. *Management Science* (forthc.).

Regarding the question of firms (not) having established processes for cybersecurity in place, only 24% of directors indicated that their processes for the cybersecurity domain are “above average” or “excellent”, and of all domains, they deemed cybersecurity to be the one equipped with the least effective processes. Cybersecurity processes are established activities such as regular discussions about cyber risks (with or without the presence of cybersecurity specialists) and management reviews of contingency plans for the event of a data breach. The survey also reveals some variation across industries. Corporations in the IT and telecom sectors had somewhat better results than average, with 42% of directors indicating their processes are rather effective. In the materials and industrials sectors fewer than 20% of directors rated their processes for cybersecurity as effective. For the health care industry, a sector that can be described as especially vulnerable to data breach incidents, 79% of survey respondents indicated that their corporations did not have robust cybersecurity processes.

The second factor leading to boards’ poor handling of cybersecurity is insufficient expertise, according to the survey findings of Cheng and Groysberg (2017). Directors reported that risk and security are the issues they find most challenging in their role as board director. The also reported not having the necessary expertise to handle them. One director stated that boards have an insufficient understanding of the cybersecurity issue and that board members are unwilling to make room for new people who would be more knowledgeable. Another director commented that boards are given too much responsibility to oversee areas where they lack proper experience, cybersecurity included.

On the one hand these survey results shed light on the self-reported obstacles of a more practical nature that board members face when confronting cybersecurity risks. On the

other hand, it is not fully clear what explains differences across companies in the level of commitment to manage these risks.

For example, even if a few firms reported that their cybersecurity risk management is effective, Cheng et al. (2021, p. 6) report that some firms found ways to improve oversight effectiveness in the cybersecurity domain:

> Respondents who rated their oversight as more effective in this area identified several ways that their boards had sought to develop the required expertise. One risk committee chair explained that his committee had created a separate board of advisors, comprising experts in cyber risk, who worked with management and the risk committee to provide advice on the area. Others noted that their boards had appointed a new member with experience in cybersecurity to supplement the board's risk management capabilities. Still others explained that the audit/risk committee had engaged consultants to work with the committee and management to help inform the board and ensure that appropriate actions were being taken to protect against cyberattacks.

These differences between firms in the level of precautionary engagement to improve cybersecurity suggest that, instead of alleged practical hurdles imposing insurmountable constraints, underinvestment in cybersecurity risk management reflects choices by the responsible actors within corporations, some of whom have postponed dealing with the issue despite mounting evidence of need. Information asymmetry is certainly a major cause of this widespread inaction: if it is not known ex ante what precise measures are actually effective at increasing cybersecurity or if such measures are difficult to observe,

especially for actors on the outside such as shareholders, then the board might have little incentive to be proactive.

4. Privacy Risk Reporting

The Regulation 2016/679, General Data Protection Regulation, introduced the concept of the Data Protection Impact Assessment as an essential tool for the accountability of data controllers for demonstrating compliance. The California Consumer Privacy Act does not have a direct reference to a risk-based approach or to an impact assessment. However, the US National Institute of Standards and Technology (NIST) Privacy Framework includes references to privacy risk. A recent NIST report introduces a privacy risk model that is designed to provide coherent privacy risk assessments evaluating the likelihood of problematic scenarios regarding the processing of personally identifiable information.[41] Thus, data protection and privacy risk assessment requirements applicable to compliance apply to the US and the EU context. Company reporting practices increasingly reflect recognition of data protection and privacy risk. A 2020 study shows that 89% of Fortune 100 companies disclosed that they included a focus on cybersecurity risk in the oversight section of their proxy statement and 99% of the companies listed data privacy in their risk factor disclosure.[42] The following two sections further discuss privacy risk reporting by firms in the US and in the EU.

[41] NIST 2020. Privacy Framework: A Tool For Improving Privacy Through Enterprise Risk Management. 16 January. Available at: https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf

[42] Klemash, S.W., Smith, J.C., and Seets, C., 2020. What Companies are Disclosing About Cybersecurity Risk and Oversight. Harvard Law School Forum on Corporate Governance. 25 August. Available at: https://corpgov.law.harvard.edu/2020/08/25/what-companies-are-disclosing-about-cybersecurity-risk-and-oversight/

4.1. Privacy Risk Reporting for Corporations in the US: SEC rules

The Division of Corporate Finance of the U.S. Securities and Exchange Commission (SEC) first published cybersecurity disclosure guidance on October 13, 2011 and the latest version of the guidance has the applicable date of 26 February 2018.[43] The guidance emphasizes that "the investing public and the U.S. economy depend on the security and reliability of information and communications technology, systems, and networks" as the reason cybersecurity is vital.[44] The guidance also highlights that company insiders who have access to information regarding a cybersecurity incident cannot trade the companies' securities before this information becomes public.[45] It requires companies to adequately disclose material data protection risks they face in a timely and periodic manner, clarifying that such risk occurs when a reasonable investor would consider the information relevant for making an investment decision and includes the possibility of harm (due to that incident) on the company's reputation, financial performance, and customer and vendor relationships, as well as the possibility of litigation or regulatory investigations or actions.[46] In the 2011 version of the guidance, the SEC emphasized that companies should "avoid generic 'boilerplate' disclosure," but also that the companies should not compromise their cybersecurity through disclosure.[47] Empirical research shows that data protection risk disclosures give investors a indication of companies' cybersecurity awareness and that the market reacts to the level of such

[43] Securities and Exchange Commission, 17 CFR Parts 229 and 249, [Release Nos. 33-10459; 34-82746] Commission Statement and Guidance on Public Company Cybersecurity Disclosures. Available at: https://www.sec.gov/rules/interp/2018/33-10459.pdf
[44] Ibid.
[45] Ibid.
[46] Securities and Exchange Commission, 17 CFR Parts 229 and 249, [Release Nos. 33-10459; 34-82746] Commission Statement and Guidance on Public Company Cybersecurity Disclosures. Available at: https://www.sec.gov/rules/interp/2018/33-10459.pdf
[47] Division of Corporation Finance, Securities and Exchange Commission, CF Disclosure Guidance: Topic No. 2 Cybersecurity Available at: https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

awareness.[48] However, research also suggests that the SEC requirement might be incentivizing companies to report insignificant risks as well as significant ones and that therefore the requirement might be creating a less reliable information environment.[49] Critics argue the regulation places an additional procedural burden on companies without effectively mitigating investor risk.[50] They also state that forcing companies to disclose their vulnerabilities places them at a disadvantage vis-à-vis cybercriminals.[51]

From the EU perspective, the General Data Protection Regulation[52] is relevant to requirements governing disclosure of data breach risk.[53] EU Market Abuse Regulation also requires companies to disclose any insider information if the information would have significant effect on the share price of the company and some cybersecurity incidents might fall within this definition.[54] Article 33 and Recital 85 of the GDPR refer to the data breach notification requirements, stating that the "controller should [report] the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to

[48] Berkman, H., Jona, J., Lee, G. and Soderstrom, N., 2018. Cybersecurity awareness and market valuations. Journal of Accounting and Public Policy, 37(6), pp.508-526.
[49] Li, H., No, W.G. and Wang, T., 2018. SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. International Journal of Accounting Information Systems, 30, pp.40-55. For example, it would be interesting to pinpoint how far a company needs to go in order to identify all potential data protection risks. A recent study refers to a complex methodology for identifying cyberattacks early using machine learning methodology with information retrieval techniques for analyzing the content of hacker forums as well as IRC channels. See Benjamin, V., Li, W., Holt, T. and Chen, H., 2015, May. Exploring threats and vulnerabilities in hacker web: Forums, IRC and carding shops. In Intelligence and Security Informatics (ISI), 2015 IEEE International Conference on (pp.85-90). IEEE.
[50] Ferraro, M.F., 2013. Groundbreaking or Broken; An Analysis of SEC Cybersecurity Disclosure Guidance, Its Effectiveness, and Implications. *Albany Law Review*, *77*, pp.297-347.
[51] Trope, R.L. and Hughes, S.J., 2011. The SEC Staff's Cybersecurity Disclosure Guidance: Will It Help Investors or Cyber-Thieves More. *Bus. L. Today*, p.1.
[52] 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)
[53] Marcogliese, P. and Mukhi R., 2018. Untangling the Tangled Web of Cybersecurity Disclosure Requirements: A Practical Guide. 17 June. Available at: https://corpgov.law.harvard.edu/2018/06/17/untangling-the-tangled-web-of-cybersecurity-disclosure-requirements-a-practical-guide/
[54] Ibid.

demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons." GDPR refers to the Data Protection Impact Assessment requirement thus: "In order to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk."[55] The Working Party 29 issued guidelines on determining high risk activities in order to facilitate the decision-making process for companies.[56]

The EU GDPR avoids the risk created by the SEC because it requires companies to make data protection risk factors public that have not yet come to the attention of hackers by requiring firms to complete an internal risk assessment document that usually is audited by experts to test compliance with the regulation. This might be a better means to incentivize the firms to assess data protection risk at an early stage and create risk-mitigation plans. However, making the risk information publicly available, as the SEC requires, may benefit the market. This suggests that using select elements from the US and EU systems in combination may address the problems of each system. The following three-step approach would be an effective means to implement such a system: (1) guidelines to determine a high-risk threshold, (2) requiring companies to create a data protection risk assessment report to be audited independently, and (3) advising companies to focus on disclosing high-risk cybersecurity incidents.

[55] Regulation (EU) 2016/679 GDPR.
[56] Article 29 Data Protection Working Party Guidelines on DPIA and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.

4.2. Privacy Risk Reporting for Corporations in the EU

GDPR Recital 85 describes the risks associated with a personal data breach as follows: “physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorized reversal of pseudonymization, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.” GDPR Article 35 states that if a type of data processing is likely to result in a high risk to the rights and freedoms of natural persons, the data controller entity shall carry out a DPIA before processing the personal data. DPIAs are an essential part of risk assessment in several organizations. Among Fortune 100 companies, 24% reported privacy as an individual risk factor when referring to fast-evolving data protection regulations that create financial risk and reputational risks in their IRS Form 10-K filings.[57]

WP 29 Guidelines analyze the personal data breach definition under the GDPR. Article 4/12 defines a data breach as a breach of security leading to accidental or unlawful destruction, loss, alteration, and unauthorized disclosure of or access to personal data transmitted, stored, or otherwise processed. Destruction of the data means the data no longer exists, while loss of personal data could refer to instances where data still exists but the controller has lost access. The latter occurs when cybercriminals use ransomware to encrypt data, if the company does not have a copy of the data they can access.[58]

[57] Klemash, S.W., Smith, J.C., and Seets, C., 2020. What Companies are Disclosing About Cybersecurity Risk and Oversight. Harvard Law School Forum on Corporate Governance. 25 August. Available at: https://corpgov.law.harvard.edu/2020/08/25/what-companies-are-disclosing-about-cybersecurity-risk-and-oversight/

[58] Article 29 Data Protection Working Party 29, 18/EN, Guidelines on Personal data breach notification under Regulation 2016/679, Adopted 3 October 2017, Revised and Adopted on 6 February 2018.

5. Economic Risk from Non-Compliance

Industry reports indicate that corporations are highly vulnerable to cyber risk.[59] The losses imposed via exposure to such risks will likely continue to increase if corporations do not change their approach to this issue. Kaspersky Lab, a technological consultancy, surveyed almost 6,000 firms across 29 countries in 2018 regarding privacy risks in the business environment. According to this survey 42% of large enterprises and 46% of small and medium-sized companies had experienced at least one data breach at some point in their company history.[60] The survey results also indicate that personal data from customers had been stolen in 40% of those data breach cases.

The Ponemon Institute and IBM Security surveyed over 400 corporations from 13 countries in 2017. Results indicated that the average organizational cost of a data breach was $7.35 million USD in the United States and $3.62 million USD across the countries where the study took place.[61] In some jurisdictions firms may face class-action lawsuits on top of these costs. For large breaches settlements can reach over $100 million USD.[62] Furthermore, the price of stocks of affected companies declines by 5% on average following the disclosure of data breach events.[63] Besides these financial costs, the Kaspersky Lab survey found that 31% of corporations that faced a data breach stated that it required them to lay off staff.

[59] Lehuedé, H., 2019. Corporate governance and data protection in Latin America and the Caribbean. Production Development series, No. 223 (LC/TS.2019/38), Santiago, Economic Commission for Latin America and the Caribbean (ECLAC).
[60] Kaspersky Lab (2018). From data boom to data doom - The risks and rewards of protecting personal data. Available at: https://go.kaspersky.com/rs/802-IJN-240/images/Kaspersky_Lab_Business%20in%20a%20data%20boom.pdf
[61] Ponemon Institute and IBM Security, 2017. Cost of Data Breach Study - Global Overview. Available at: https://www.securityupdate.net/SU/IBMSecurity/IBM-Security-Cost-of-Data-Breach-Study.pdf
[62] Southwell, A. H., 2017. Gibson Dunn Reviews U.S. Cybersecurity and Data Privacy. Columbia Law School Blue Sky Blog. Available at: http://clsbluesky.law.columbia.edu/2017/02/03/gibson-dunnreviews-u-s-cybersecurity-and-data-privacy/
[63] Ponemon Institute, 2017. The Impact of Data Breaches on Reputation and Share Value. Available at: www.centrify.com/media/4772757/ponemon_data_breach_impact_study_uk.pdf

At the same time, it is noted that the economic fallout of noncompliance with privacy rules due to regulatory fines and sanctions was much less than anticipated because of the enforcement difficulties privacy laws create. Companies could have gotten the impression that the GDPR's level of enforcement was low. This may have reflected low enforcement commonly expected in the early years of a law's adoption. Indeed, there are indications that enforcement is increasing as the law's principles gradually are translated into more precise requirements throughout the European legal system.

Furthermore, Jang and Newman (2021) observed, transnational civil society groups are emerging across Europe. They argued these groups may create what they called a "transnational fire alarm" system will spur and support litigation against corporations' infringements of privacy rights. Individual consumers are often ill-positioned to bargain for privacy ex ante or to react to privacy harms. Civil society organizations may be able to address this limitation, thereby deterring corporate abuses.

On the other hand, other scholars do think that privacy laws in their current form are insufficient for deterring corporations from underinvesting in privacy risk management, which means that firms will find overall costs due to privacy law enforcement manageable, and that the field remains tilted against individuals concerned about their privacy despite the hype around new privacy laws. For example, Helman (2019) argues that consent mechanisms, that are typically part of newly emerging privacy laws, are insufficient and that market failures reduce corporations' incentives to internalize privacy concerns. The same article argues that data use imposes externalities on others, implying that privacy infringements can burden individuals irrespective of their conscious choice. Helman (2019) as well as Hartzog and Richards (2020) propose that social

network executives should be held accountable for breaches in data privacy protection, thus effectively demanding a fundamental reform of traditional corporate law tenets, in order to get privacy practices of companies with business models that rely on handling significant amounts of (sensitive) private data better under control.

The following table (Table 1) summarizes the results from several studies that empirically assess the impact of data breaches on firm fundamentals.

Table 1. Summary of previous empirical findings on the impact of data breaches on affected firms

Authors	Findings
Cavusoglu et al. 2004	1. Breaches result in overall loss of 2.1% of value over 2 days following event 2. Breach costs are higher for internet firms 3. Costs not related to breach type 4. Breach costs increase over time 5. Negative correlation between size and stock market response
Hovav & D'Arcy 2003	1. Breach costs higher for Internet firms 2. No overall significant market impact for denial of service attacks
Garg et al. 2003	1. Security attacks result in overall loss of 5.3% of value over 3-day event window 2. Internet security vendors experience positive returns of 10.3% over the same window when security attacks are reported 3. Property–casualty insurers experience a loss of 2.0% over the same window when security attacks are reported
Campbell et al. 2003	1. Breaches result in no statistically significant loss for entire sample 2. Breaches involving unauthorized access to customer personal data or firm proprietary data result in an average loss of firm value of 5.5%
Gatzlaff & McCullough 2010	1. Negative association between market reaction and firms that are less forthcoming about the details of the breach 2. Firms with higher market-to-book ratios experience greater negative abnormal returns associated with a data breach 3. Firm size and subsidiary status mitigate the negative effect of a data breach on the firm's stock price and the negative market reaction to a data breach is more significant in the most recent time periods of the sample

Source: Based on Gatzlaff and McCullough (2010); Frimpong and Chen (2021)

6. Cases of Legal Complaints in the Aftermath of Data Breaches

Less visible and smaller magnitude data breaches that do not attract a lot of public attention might not lead to shareholders starting class action litigation.[64] However, high-visibility data breaches have led to many instances of such shareholder class action suits being put forward. Companies targeted by such suits occasionally succeeded to navigate and react to the challenge by responding with motions to dismiss and through settlement. But as the stakes are getting higher in the case of large-scale data breaches, lawyers hired by the shareholders are improving their strategies and refining their pleadings to overcome deficiencies of their earlier legal strategies.

Given recent cases, corporations are increasingly aware of the possibility of being targeted with shareholder class action suits after data breaches. It will be seen moving forward if the threat of such litigation affects corporations' level of commitment to robust cybersecurity risk management practices.

In the following, prominent case examples of lawsuits spurred by data breaches will be discussed, focusing first on cases in the US (Section 6.1.) and next on the European context (Section 6.2.). While for the US the discussion will center of class action lawsuits brought by shareholders, in the European setting group action brought against firms in the aftermath of data breaches rests on consumer initiatives and hence those will be primarily discussed.

[64] Hooker, M. and Pill, J., 2016. You've Been Hacked, and Now You're being Sued: The Developing World of Cybersecurity Litigation. (August), 90 Florida Bar Journal 30.

These cases illustrate the economic damage that corporations in some instances suffer because of mismanagement of privacy risk and the related potential penalties for non-compliance. It should be noted that not only these direct costs are relevant but also indirect reputational cost for the brand name. Even with such costs becoming more evident with time, problems of information asymmetry between shareholders and management can stand in the way of corporations investing in more prudent privacy risk management practices.

6.1. Examples from the US

Before we now turn to the US case examples it shall be noted that legal scholars remark that shareholder litigation after data breaches face considerable legal obstacles. One concern is that these class action suits are plagued by standing problems because the circuit is split on what constitutes injury from a data breach.[65] After a company's stock price declines following a data breach, shareholders pursuing securities fraud class action suits find it difficult to show that they acted upon to their detriment on a firms' material misrepresentations contained in public statements and 10-K filings. Additionally, derivative shareholder lawsuits that aim at boards and directors for alleged breach of fiduciary duties are hard to substantiate since a high bar was set for successfully pleading demand futility and given the power of the business judgment rule in Delaware courts.[66]

Shareholder class actions in the privacy domain are an example of the emerging pervasiveness of so-called event-driven securities litigation, in which investors sue when a corporation's share price falls in response to a corporate shock, such as a product

[65] Dowty, M., 2017. Life Is Short. Go to Court: Establishing Article III Standing in Data Breach Cases. S. Cal. L. Rev., 90, pp.683-718.
[66] Marcus, D.J., 2018. The Data Breach Dilemma: Proactive Solutions for Protecting Consumers' Personal Information. *Duke LJ*, *68*, pp.555-593.

liability crisis, a sexual harassment scandal, oil spill, or, in line with the focus of the present article, a data breach.

6.1.1. SolarWinds

A shareholder class action lawsuit was filed against SolarWinds regarding the fall in the price of shares observed after a hack disclosed in December 2020. Shareholders alleged that they were damaged because SolarWinds failed to rapidly disclose vulnerabilities that could lead to the exposure of thousands of customers. SolarWinds is a U.S. based corporation that develops software for organizations which is used to manage their networks, systems, and IT infrastructure.

The plaintiffs argue that SolarWinds, including previous CEO Kevin Thompson and CFO J. Barton Kalsu "failed to employ adequate cybersecurity safeguards and did not maintain effective monitoring systems to detect and neutralize security breaches" and that these failures left the company and its customers "particularly susceptible to cyber-attacks."[67]

A Reuters article from December 2020 reported that SolarWinds had been notified already in 2019 by a security researcher who stated that anyone could obtain access to SolarWinds' update server by using the password "solarwinds123."[68] SolarWinds accepted that Orion, its main network management software, had served as conduit for a cyberespionage operation. The hackers introduced malicious code into Orion software

[67] Scmagazine, 2021. SolarWinds lawsuits merge as stockholders begin documenting financial losses. 12 March. Available at: https://www.scmagazine.com/news/breach/solarwinds-lawsuits-merge-as-stockholders-begin-documenting-financial-losses

[68] Satter, R., Bing, B, Menn, J., 2020. Hackers used SolarWinds' dominance against it in sprawling spy campaign. Reuters. 16 December. Available at: https://www.reuters.com/article/global-cyber-solarwinds/hackers-used-solarwinds-dominance-against-it-in-sprawling-spy-campaign-idUSKBN28Q07P

updates received by almost 18,000 customers, including U.S. Treasury and Department of Commerce.[69]

Following the first Reuters report on December 13, 2020 SolarWinds' shares fell 17%. A few days after the Reuters article mentioning the weak password came out and SolarWinds' shares fell another 8%. Shareholders allege that SolarWinds' disclosures reflected in the 2019 Form 10-K and Form 10-Qs for the first three quarters of 2020 were materially false, misleading and insufficient since they did not properly discuss the substantial cybersecurity risk to the company and its clients generated by SolarWinds' vulnerabilities.

6.1.2. Ubiquiti

Another recent instance that comes to mind is a recent data breach that concerned a provider of Internet of Things and networking equipment devices that services across industries and goes under the name of Ubiquiti. Ubiquiti, which has its headquarters in New York, produces and sells wireless data communication equipment as well as wired products for homes and enterprises.

In early January 2021, the company began notifying customers regarding an unauthorized access issue or intrusion detected on the management services for Ubiquiti systems. A few months later, it became clearer that the impact of the unauthorized access was larger in scope than initially thought, and included private cryptographic

[69] Ibid.

encryption keys, databases, loss of root credentials for cloud services affecting thousands of direct and indirect clients.[70]

A shareholder class action complaint was filed alleging that Ubiquiti made materially false and/or misleading declarations and/or failed to reveal that: first, the firm had downplayed the scope and severity of the data breach in January 2021; second, attackers had obtained administrative access to Ubiquiti's servers and obtained access to vast amounts of information, including all databases, all credentials in the user database, and sensitive company information needed for the forging of single sign-on (SSO) cookies; third, as a result, intruders had obtained access to credentials allowing to remotely access Ubiquiti's customers' systems; and four, in light of these facts and occurrences, Ubiquiti's previously made positive statements about the corporation's operations, business, and future prospects were materially misleading and/or lacked a reasonable basis.[71]

6.1.3. Marriott

Marriott reported two separate massive data breaches in 2018 and then again in 2020. Marriott is a US-based multinational company that operates, franchises, and licenses lodging covering hotel, residential, and timeshare properties.

The breach reported in 2018 had already started four years earlier in 2014 and went unnoticed for several years, ultimately leading to personal data of over 300 million guests leaking, including guests' names, email addresses, phone numbers, passport numbers,

[70] Clark, M., 2021. Ubiquiti is accused of covering up a 'catastrophic' data breach — and it's not denying it. The Verge. 31 March. Available at: https://www.theverge.com/2021/3/31/22360409/ubiquiti-networking-data-breach-response-whistleblower-cybersecurity-incident

[71] Businesswire, 2021. Ubiquiti Investors: July 19, 2021 Filing Deadline in Class Action. 11 June. Available at: https://www.businesswire.com/news/home/20210611005074/en/UBIQUITI-INVESTORS-July-19-2021-Filing-Deadline-in-Class-Action-%E2%80%93-Contact-Lieff-Cabraser

arrival and departure information, VIP status, and loyalty program numbers. Also, eight million credit card records were leaked. The breach reported in March 2020 involved personal data of 5,2 million guests getting stolen by unauthorized intruders.

Affected parties launched legal complaints against Marriott both in the US and in the UK.

First, the US cases involving Marriott. With respect to the breach reported in 2018, securities and derivative suits class action suits brought against Marriott in the US by shareholders were both dismissed in 2021. It was reasoned that the shareholders failed to adequately allege that Marriott made misleading statements about the data breach, according to the U.S. District Court for the District of Maryland. Further, Judge Paul W. Grimm held that the shareholder behind the derivative suit did not meet pre-suit demand requirements.[72]

Regarding the breach reported in 2020, a data breach class action invoking the CCPA brought against Marriott by consumers in the US was dismissed in early 2021 on standing grounds.[73] Another attempt at a consumer class action suit against Marriott over the breach revealed in 2020 failed on standing grounds, as U.S. District Judge Paul Grimm noted in a March 2021 ruling that the shareholders had not sufficiently shown that their claimed injuries were “fairly traceable to Marriott’s conduct.”[74]

[72] Bennett, J., 2021. Marriott Beats Investor Class, Derivative Claims on Data Breach. Bloomberg Law. 14 June. Available at: https://news.bloomberglaw.com/securities-law/marriott-beats-investor-class-derivative-claims-on-data-breach

[73] Brennan, T. and Mayant, L., 2021. Dismissal Of Marriott Data Breach Lawsuit Shows How Plaintiffs Still Face Standing Hurdles In The Post-CCPA Era. Jdsupra. 28 January. Available at: https://www.jdsupra.com/legalnews/privacy-minded-dismissal-of-marriott-8256692/

[74] Merken, S., 2021. Judge tosses lawsuit over Marriott's 2020 data breach. Reuters. 4 March. Available at: https://www.reuters.com/article/dataprivacy-marriott-idUSL2N2L21IQ

However, Marriott also faced data breach related legal repercussions in the UK. Regarding the breach reported in 2018, Marriott was ultimately fined £18.4 million in 2020 by the Information Commissioner's Office (ICO), the UK's data privacy watchdog.[75] Also regarding the breach reported by Marriott in 2018, a consumer class action lawsuit was started in London's High Court in late 2020 under the lead of Martin Bryant, a technology journalist, on behalf of millions of hotel guests from England and Wales who made reservations at hotel brands owned by Marriott International.[76] The dates of Marriott's first large data breach make it fall under GDPR, since the new EU privacy law came into application in May 2018. The lawsuit claims that the hotel chain failed to take adequate technical or organizational measures to ensure the security of guests' personal data and to prevent unauthorised and unlawful processing of that data.

6.1.4. Equifax

Equifax is a US-based multinational firm active in the domain of consumer credit reporting, and it is one of the three largest firms in this domain, besides Experian and TransUnion. Evidently, this business domain involves the collection of vast amounts of personal data on consumers worldwide. Equifax was hacked in 2017 with this data breach leading to the exposure of personal information of nearly half of the US population, more than 143 million US citizens, including consumers' names, addresses, driver's license numbers, social security numbers, and birth dates.[77]

[75] Tidy, J., 2020. Marriott Hotels fined £18.4m for data breach that hit millions. BBC News. 30 October. Available at: https://www.bbc.com/news/technology-54748843
[76] Croft, J., 2020. Hotel group Marriott faces London lawsuit over huge data breach. Financial Times. 19 August. Available at: https://www.ft.com/content/d6202d00-a173-4b15-b68a-46764934c76b
[77] Hayes, P., 2020. Equifax's $149 Million Data Breach Settlement OK'd. Bloomberg Law. 27 February. Available at: https://news.bloomberglaw.com/securities-law/equifaxs-149-million-data-breach-securities-settlement-gets-ok

A group of shareholders that had bought Equifax securities in 2016 and 2017 filed a class action lawsuit against the company and corporate officers. These shareholders alleged that due to false or misleading statements and omissions about the breach by Equifax the share price got artificially inflated followed by share price declines by nearly 17% after the company revealed the data breach. Shareholders also alleged that Equifax failed to take the most basic precautions to secure its databases.

Equifax had made public statements regarding its effort to ensure the protection of personal consumer data and installing internal controls.[78] The company representatives had stated that they "regularly review and update [their] security protocols to ensure that they continue to meet or exceed established best practices at all times.[79] The court found that these statements were not mere opinions and they related to a core aspect of Equifax's business, so it was likely investors would rely on these decisions."[80] Meanwhile, according to Congress the data breach was entirely preventable and Congress criticized Equifax for a "history of 'laughably bad' security measures, a 'lack of accountability' within its management, and a 'complex and antiquated' IT system."[81] Furthermore, allegedly Equifax used the word "admin" as both password and username for a portal used to manage credit disputes and that contained sensitive information.[82]

In response to the lawsuit, Equifax filed a motion to dismiss the complaint. A January 2019 court ruling granted a part of the motion and denied another part. The "court upheld

[78] Klaus, T. and Elzweig, B., 2020. The impact of data breaches on corporations and the status of potential regulation and litigation. *Law and Financial Markets Review*, *14*(4), pp.255-260.
[79] In re Equifax Inc. Sec. Litig., 357 F. Supp. 3d 1189, 1223 (N.D. Ga. 2019).
[80] Ibid, 1224.
[81] Ibid, quoting Staff of S. Permanent Subcomm. on Investigations of the S. Comm. on Homeland Security and Governmental Affairs, 116th Cong., Rep. on How Equifax Neglected Cybersecurity and Suffered a Devastating Data Breach 6 (2019).
[82] Wolff-Mann, E., 2019. Equifax used 'admin' as username and password for sensitive data: lawsuit. Yahoo Finance. 18 October. Available at: https://finance.yahoo.com/news/equifax-password-username-admin-lawsuit-201118316.html

the plaintiff's 'multitude of specific, detailed factual allegations demonstrating that Equifax's systems were grossly deficient and outdated, below industry standards, and vulnerable to attack.'"[83] However, the "plaintiff's claims that Equifax had been obligated to disclose details of the breach sooner were dismissed."[84]

In mid-2020 the shareholder class action lawsuit ended in a settlement to the amount of $149 million after a Georgia federal district judge gave final approval. Judge Thomas W. Thrash Jr. certified the settlement, according to filings of the U.S. District Court for the Northern District of Georgia. Equifax did not admit wrongdoing as part of the settlement.[85]

This large settlement of $149 million is only one of several sums Equifax had to pay due to the 2017 data breach. The reason is that the corporation's shareholders were not the only affected party pursuing the legal route. In connection with a class-action brought by affected customers, Equifax agreed to pay at least $650 million, with $275 million destined to cover state and federal fines.

Klaus and Elzweig (2020) note that the Equifax breach led to the largest settlement in a case involving a security breach, and that the second highest settlement, which obtained in a case against Uber, corresponded to one-fourth of the Equifax settlement amount.[86]

[83] Stubbs, M., 2020. Equifax Agrees to $149 Million Settlement for Infamous 2017 Data Breach. Expert Institute. 25 June. Available at: https://www.expertinstitute.com/resources/insights/equifax-agrees-to-149-million-settlement-for-infamous-2017-data-breach/
[84] Ibid.
[85] Bennett, J., 2020. Equifax, Investors Get Final OK of $149 Million Hack Settlement. Bloomberg Law. 2 July. Available at: https://news.bloomberglaw.com/us-law-week/equifax-investors-get-final-ok-of-149-million-hack-settlement
[86] Pietsch, B., 2019. Factbox: Biggest U.S. Data Breach Settlements before Equifax. Reuters. 22 July. Available at: https://www.reuters.com/article/us-equifax-cyber-settlement-factbox-idUSKCN1UH22P

Overall, Equifax is thus far culpable for over $1 billion settlement expenses, which could be read as a sign of legal enforcement of liability for cybersecurity slowly strengthening, especially for companies handling large amounts of sensitive data, which makes them targets for cyberattacks.[87]

6.1.5. Heartland

In one of the early cases in the US, Heartland, a payment processing and technology provider, faced a shareholder securities fraud class action lawsuit after a large data breach became public in 2009 that had compromised information about at least 130 million credit or debit cards, including information like expiration dates, and 650 financial service companies. Most of the breach itself had apparently occurred the year prior in 2018.[88] The price of Heartland shares declined by almost 80% following the announcement of the breach, prompting shareholders to bring the suit against Heartland.

The plaintiffs claimed that the firm had hidden the attack on its network for a long period of time - Heartland disclosed the breach a year after it had happened - and exaggerated its level of preparedness. Shareholders alleged that the 10-K filings (stating an emphasis on maintaining a high level of security) were misleading and created an appearance that Heartland's cybersecurity measures were more resilient than was really the case. The plaintiffs also alleged that how long it took for the company to disclose the breach implied a material omission in the firm's following statements and financial reports.[89]

[87] Ibid.
[88] The Heartland case is reminiscent of the Yahoo case of 2016, when the firm disclosed that vast data breaches had occurred in 2013 and 2014 prompting shareholders to initiate a class action securities fraud lawsuit. In that case they successfully forced Yahoo to settle for $80 million. See: Marcus, D.J., 2018. The Data Breach Dilemma: Proactive Solutions for Protecting Consumers' Personal Information. *Duke LJ*, *68*, pp.555-593.
[89] Klaus, T. and Elzweig, B., 2020. The impact of data breaches on corporations and the status of potential regulation and litigation. *Law and Financial Markets Review*, *14*(4), pp.255-260.

Interestingly the case was ultimately dismissed.[90] The court argued that Heartland's failure to disclose the cyber-attack earlier did not constitute a material omission. The court also held that the mere fact that the system had been penetrated did not necessarily mean that the companies' public statements were untruthful.[91] Thus, the opinion reflected the idea that suffering a breach does not automatically demonstrate insufficient effort at maintaining a high level of security. Instead, the notion was implied that there is plausibility to hackers overcoming a firm's security systems despite of a firm exercising high cybersecurity effort.

The Heartland case signals that potential litigants face a relatively high burden of proving actual material misrepresentations or omissions regarding a corporation's security systems, and that it is usually insufficient to merely rely on general allegations of security inadequacies after the occurrence of a data breach.[92]

6.2. Examples from the EU

The class action model originated in the US and continues to be predominantly a US occurrence, however, Canada, as well as several European countries relying on civil law, have introduced some changes in recent years allowing consumer organizations representing groups of consumers to bring claims on their behalf. While we cannot speak

[90] While the shareholder class action against Heartland was dismissed, the company and its officers and directors had to pay $60 million, $41.4 million, and $2.4 million in settlements with Visa, MasterCard, and American Express respectively, besides up to $2.4 million in the context of a consumer cardholder class action, as well as costs related to internal investigations and defense costs of the dismissed lawsuit. See: Trautman, L.J. and Altenbaumer-Price, K., 2010. The board's responsibility for information technology governance. *J. Marshall J. Computer & Info. L.*, *28*, pp.313-342.

[91] Skedsvold, M.C., 2018. A Duty to Safeguard: Data Breach Litigation Through a Quasi-Bailment Lens. *J. Intell. Prop. L.*, *25*, pp.201-226.

[92] Marcus, D.J., 2018. The Data Breach Dilemma: Proactive Solutions for Protecting Consumers' Personal Information. *Duke LJ*, *68*, pp.555-593.

of US-style class actions in a strict sense, in Europe new forms of collective redress are emerging, also in the privacy domain and in connection with the GDPR.

6.2.1 Article 80 of GDPR and Collective Redress for Consumers

A recommendation in 2013 by the Commission of the European Union suggests to Member States that they introduce some type of collective redress for consumers.[93] One notable difference to the US is that it is recommended in Europe that solely not-for-profit (consumer) associations should qualify to represent a class.[94]

The GDPR also follows this idea and endorses that collective redress should be an option for data subjects under the GDPR. However, Member States should be free to decide whether collective redress will be available for claims seeking damages, or only in the context of non-monetary judicial remedies.[95] Data breach typically affects a multitude of individuals in a similar fashion, and a collective redress becomes a straightforward option for them to seek remedy for their injury. If permitted to be combined with non-economic damages, e.g. emotional stress, then the opportunity to pursue collective redress could influence the legal environment in a jurisdiction and increase the risks from litigation for companies suffering a data breach.[96]

Now we take a look whether the newly created channels for non-profit third-party organizations to assist in collective redress actions - as stipulated by Art. 80 of GDPR – de facto spurred a new round of NGO-supported privacy related complaints.

---

[93] European Commission Recommendation 2013/396/EU. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013H0396&from=EN
[94] Ibid, paragraph III.4 (a).
[95] Art. 80 and Whereas-clause 142 of the GDPR.
[96] Though not all Member States permit damages to be claimed in collective redress efforts. E.g., collective redress efforts regarding privacy in Germany and France will not cover compensation for damages suffered but merely for injunctive relief.

While the media has often highlighted the significant penalties that GDPR created - reaching up to 20 million euro or 4 per cent of a company's annual world-wide revenue - at the same time doubts were raised regarding enforcement and implementation problems. The latter could arise due to the high technicality of the law, to the complicated legal language used, and to the complexity of the consent process.[97] On top of this comes the problem that when a multitude of individuals gets affected by a data breach this gives rise to collective action problems for bottom-up complaints to be organized, making it difficult for them to exercise their privacy rights afforded by the GDPR**.**

Here, Art. 80 of GDPR can assist towards a solution. Article 80 allows third parties with a public interest-focused mission and active in the data protection domain the right to bring complaints on behalf of affected individuals. Based on this, several data protection NGOs, consumer protection bodies, and civil liberties organizations can file complaints on behalf of European citizens.[98] According to a multi-stakeholder survey sponsored by the European Commission, 13 NGOs had made use of Article 80 in the first implementation year of the law.[99] Among them were BEUC (Belgium), Consumentenbond (Netherlands), dTest (Czech Republic), Ekpizo (Greece), Federacja Konsumentow (Poland), Forbrukerradet (Norway), LQDN (French), Noyb (Austria), Panoptykon Foundation (Poland), Privacy International (UK), Sveriges Konsumenter (Sweden), Verbraucherzentrale Bundesverband (Germany), and Zveza Postrosnikov Slovenije (Slovenia).

[97] Jang, W. and Newman, A.L., 2021. Enforcing European Privacy Regulations from Below: Transnational Fire Alarms and the General Data Protection Regulation. *JCMS: Journal of Common Market Studies*, (forthcoming).
[98] Ibid.
[99] Multistakeholder Group, 2020. Contribution from the Multistakeholder Expert Group to the Commission 2020 Evaluation of the General Data Protection Regulation. Brussels, 17 June.

Particularly high-profile initiatives were led with the support of the Austrian-based Noyb[100] and the French-based LQDN, which resulted in considerable financial penalties being imposed on the involved companies.

In 2018 in GDPR's early days, Noyb and LQDN gathered over 9,000 individuals to participate in an Art. 80 action against Google. The case was filed with CNIL - the French data protection authority - and raised the concern that Google's personalized ad system was problematic with respect to its lack of consent and transparency.[101] This resulted in CNIL imposing 50 million Euro fine on Google and calling for the issues to be remediated.[102]

A different case, brought by the Norwegian Consumer Council (Forbrukerradet) and Noyb, involved a complaint against the dating app Grindr for illegally sharing sensitive personal user data with advertising companies. In a decision issued in January 2021, the Norwegian Data Protection Authority ruled in favor of the complaint and levied a fine of close to 10 million Euro on Grindr.

These early developments suggest that the model envisioned by Art. 80 of GDPR of permitting not-for-profit organizations to assist European citizens in the pursuit of collective redress actions can at times effectively mobilize bottom-up efforts, sometimes even involving pan-European coordination, that end up contributing towards European privacy law enforcement.

[100] Noyb is the NGO linked to privacy activist Max Schrems.
[101] Jang, W. and Newman, A.L., 2021. Enforcing European Privacy Regulations from Below: Transnational Fire Alarms and the General Data Protection Regulation. *JCMS: Journal of Common Market Studies*, (forthcoming).
[102] CNIL, 2019. SAN-2019-001. Available at: https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf

6.2.2. British Airways

Between end of August 2018 and beginning of September 2018, hackers carried out an operation on the website of British Airways, with this web skimming attack affecting thousands of transactions, causing the personal data of about 430,000 staff and customers to be leaked, including credit card data. A ICO investigation concluded that sufficient security measures, e.g. multi-factor authentication, were not in place which led to vulnerability.

The company was later fined £20 million by the UK's Information Commissioner's Office (ICO). The fine is noticeably smaller than the £183 million (1.5% of turnover) that the ICO initially said it intended to impose back in 2019. It was stated that the economic impact of Covid-19 played a role in reducing the fine amount. Still, it is the largest penalty issued by the ICO to date. This was the first major fine issued by the commissioner under the GDPR and was therefore being watched closely by a European audience recognizing that it could be a potential landmark decision. European privacy activists had not expected the fine to be so much lower than the original amount envisaged by ICO in 2019.[103]

Besides the ICO fine, British Airways also was confronted with group action by affected individuals. It would become the largest ever group-action personal-data claim in the UK, with more than 16,000 affected individuals involved. The claim by the solicitors seeks damages for financial loss, including bank charges; but also for "distress and inconvenience" including from having to "change credit cards and change passwords to

[103] Tidy, J., 2020. British Airways fined £20m over data breach. BBC News. 16 October. Available at: https://www.bbc.com/news/technology-54568784

various online accounts." It also states that some claimants have been targeted by scam emails and possibly had their creditworthiness negatively affected.[104]

In mid-2021 British Airways settled with the litigants over a confidential amount and with the settlement not including any admission of liability. Since the terms of the settlement are kept confidential, it is unknown how many of the 16,000 will obtain a payout or what total amount the airline agreed to pay.[105]

6.2.3. Amazon

A recently disclosed significant fine levied by a European regulator against Amazon could open up a discussion of how the European and US privacy regimes might potentially interact in the future in unexpected ways.

The price of Amazon shares dropped by as much as 8% on Friday, 30 July 2021, after the e-commerce company disclosed a significant fine issued by the Luxembourg National Commission for Data Protection for allegedly failing to comply with European privacy laws and after it posted lesser than expected second-quarter earnings.[106]

The disclosure occurred via a US Securities and Exchange Commission (SEC) filing. The revealed fine amounts to $885 million (746 million euros) and was imposed on July

[104] Solicitors' claim, 2020. MR STEPHEN WEAVER & OTHERS (Claimants) against BRITISH AIRWAYS PLC (Defendant). Available at: https://files.lbr.cloud/public/2020-06/BA%20particulars%20of%20claim.pdf?BrAt.nnYUI75cuvkZ2oOSF8d7fM9HWLc

[105] BBC News, 2021. British Airways data-breach compensation claim settled. 6 July. Available at: https://www.bbc.com/news/technology-57734946

[106] Ponciano, J., 2021. Amazon Stock Loses $130 Billion In Market Value After $885 Million Fine And Disappointing Earnings Report. Forbes. 30 July. Available at: https://www-forbes-com.cdn.ampproject.org/c/s/www.forbes.com/sites/jonathanponciano/2021/07/30/amazon-stock-loses-130-billion-in-market-value-after-885-million-fine-and-dismal-earnings-report/amp/

16 on the grounds that Amazon's processing of personal data was non-compliant with the GDPR.[107] It waits to be seen if the ultimately levied fine will remain such a high figure.

This is so far – by a wide margin - the largest fine since the law started to be applied in 2018. Other firms, e.g. Google, British Airways, H&M and Marriot Hotels, have received penalties from European governments for breaching privacy laws, however, in those cases fines amounted to tens, rather than to hundreds of millions.[108] The second highest fine issued under the GDPR was the 50 million Euro penalty that France imposed on Google in 2019.

Amazon stated in response via a spokeswoman that there was no related data breach event and that the issued decision and fine is without merit. Further, according to the Amazon spokeswoman, the "decision relating to how we show customers relevant advertising relies on subjective and untested interpretations of European privacy law, and the proposed fine is entirely out of proportion with even that interpretation."[109]

While this Amazon case is still unfolding it remains to be seen whether it might reach proportions where it could trigger US shareholders holding Amazon stock to file class action lawsuits in US courts against Amazon after the company's privacy infringing conduct in Europe was heavily sanctioned by a European regulator which negatively impacted the share price.

[107] Leggett, T., 2021. Amazon hit with $886m fine for alleged data law breach. BBC News. 1 August. Available at: https://www.bbc.com/news/business-58024116
[108] Ibid.
[109] Ibid.

7. Conclusion

This article discussed the potential economic impact on companies stemming from recently established privacy laws in the US and Europe coming into force and presenting additional opportunities for parties affected by a data breach to (collectively) litigate against breached firms.

It is argued in the article that information asymmetries and related agency problems between management and other corporate stakeholders are an important explanation for companies' underinvestment in cybersecurity measures. Management efforts at privacy compliance are difficult to observe and monitor which opens up opportunities for firm management to act in ways that are not in line with the preferences of shareholders and other stakeholders. High-profile class-action suits initiated after detection of privacy violations by firms and the imposition of significant penalties by regulatory authorities are signs of the potentially fraught management-shareholder relationship with regard to firms' data protection practices. The present article aimed to show, additionally, that data protection regulations, if credibly enforced, might have their own effects on corporate governance dynamics, potentially providing new incentives for managers to pay attention to privacy risks.

Looking forward, it remains to be seen if the US will move towards establishing a new Federal privacy law or if state-level privacy laws will continue characterizing the US approach. A recent proposal for creating a federal privacy law by two Republican Senators envisions to strengthen some privacy protections. At the same time, the proposed bill creates no right for consumers to sue companies, instead leaving enforcement to the Federal Trade Commission and to state attorneys general. The proposed law would also nullify state and local privacy laws. In that form the bill rather

accommodates the preferences of major technology firms and corporate lobbyists and is likely to face resistance from Democrats which in 2021 control both branches of Congress.[110]

Meanwhile, on the European side of the Atlantic a debate is happening around the EU's proposed artificial intelligence (AI) regulation which was released on 21 April 2021. The suggested law lays out a nuanced approach, banning select uses of AI, heavily regulating high-risk uses and lightly regulating lower risk AI systems. Naturally, the proposed AI regulation includes rules on data and data governance, and this foreshadows future interactions between EU privacy laws and the developing EU artificial intelligence laws. The EU regulatory approach contrasts with the piecemeal and decentralized approach to AI taken by recent administrations in the US, with responsibility to oversee AI delegated to specific regulatory agencies.[111]

The EU initiative notwithstanding, there will still be probably attempts for the US and the EU to cooperate on AI. For example, the EU Commission already provided the Biden administration with a blueprint for trans-Atlantic cooperation on this subject. However, differing regulatory philosophies—and varying structures of corporate, consumer and civil society interests—will likely put limits on trans-Atlantic cooperation. Still, pragmatism induced by economic pressures might give rise to selective mutual recognition arrangements on AI, perhaps even negotiated under the framework of a broader trans-Atlantic AI dialogue.[112]

[110] Uberti, D., 2021. GOP Bill Attempts to Inject Life Into Stalled Internet Privacy Talks. Wall Street Journal. 28 July. Available at: https://www.wsj.com/articles/gop-bill-attempts-to-inject-life-into-stalled-internet-privacy-talks-11627464601

[111] MacCarthy, M. and Propp, K., 2021. Machines Learn That Brussels Writes the Rules: The EU's New AI Regulation. Brookings. 4 May. Available at: https://www.brookings.edu/blog/techtank/2021/05/04/machines-learn-that-brussels-writes-the-rules-the-eus-new-ai-regulation/

[112] Ibid.

References

Akerlof, G.A., 1970. The Market for Lemons: Quality Uncertainty and the Market Mechanism. *The Quarterly Journal of Economics*, 84(3), pp. 488-500.

Anderson, R.J., and T. Moore, 2006. The Economics of Information Security. *Science*, 314, pp. 610-613.

Article 29 Data Protection Working Party 29, 18/EN, Guidelines on Personal data breach notification under Regulation 2016/679, Adopted 3 October 2017, Revised and Adopted on 6 February 2018.

Article 29 Data Protection Working Party Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.

BBC News, 2021. British Airways data-breach compensation claim settled. 6 July. Available at: https://www.bbc.com/news/technology-57734946

Becht, M., Bolton, P., and A. Röell, 2007. Corporate Law and Governance. In: Polinsky, A.M. and S. Shavell (eds.) *Handbook of Law and Economics - Volume 2*, Elsevier: Amsterdam, pp. 829-943.

Benjamin, V., Li, W., Holt, T. and Chen, H., 2015, May. Exploring threats and vulnerabilities in hacker web: Forums, IRC and carding shops. In Intelligence and Security Informatics (ISI), 2015 IEEE International Conference on (pp. 85-90). IEEE.

Bennett, J., 2020. Equifax, Investors Get Final OK of $149 Million Hack Settlement. Bloomberg Law. 2 July. Available at: https://news.bloomberglaw.com/us-law-week/equifax-investors-get-final-ok-of-149-million-hack-settlement

Bennett, J., 2021. Marriott Beats Investor Class, Derivative Claims on Data Breach. Bloomberg Law. 14 June. Available at: https://news.bloomberglaw.com/securities-law/marriott-beats-investor-class-derivative-claims-on-data-breach

Berkman, H., Jona, J., Lee, G. and Soderstrom, N., 2018. Cybersecurity awareness and market valuations. *Journal of Accounting and Public Policy*, 37(6), pp.508-526.

Bernheim, B.D. and M. Whinston, 1986. Common agency. *Econometrica*, 54(4), pp.923-942.

Brennan, T. and Mayant, L., 2021. Dismissal Of Marriott Data Breach Lawsuit Shows How Plaintiffs Still Face Standing Hurdles In The Post-CCPA Era. Jdsupra. 28 January. Available at: https://www.jdsupra.com/legalnews/privacy-minded-dismissal-of-marriott-8256692/

Businesswire, 2021. Ubiquiti Investors: July 19, 2021 Filing Deadline in Class Action. 11 June. Available at: https://www.businesswire.com/news/home/20210611005074/en/UBIQUITI-INVESTORS-July-19-2021-Filing-Deadline-in-Class-Action-%E2%80%93-Contact-Lieff-Cabraser

Campbell, K., Gordon, L.A., Loeb, M.P. and Zhou, L., 2003. The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer security*, *11*(3), pp.431-448.

Cavusoglu, H., Mishra, B. and Raghunathan, S., 2004. The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce*, *9*(1), pp.70-104.

Chatterjee, C. and D.D. Sokol, 2021. Data Security, Data Breaches, and Compliance. In: van Rooij, B. and D.D. Sokol (eds.) *Cambridge Handbook on Compliance*, Cambridge University Press: Cambridge, pp.936-948.

Cheng, J. Y.-J., and Groysberg, B., 2017. Why Boards Aren't Dealing with Cyberthreats. *Harvard Business Review* (digital article). February 22. Available at: https://hbr.org/2017/02/why-boards-arent-dealing-with-cyberthreats

Cheng, J. Y.-J., Groysberg, B., Healy, P. and Vijayaraghavan, R., 2021. Directors' Perceptions of Board Effectiveness and Internal Operations. *Management Science* (forthc.).

Cisco 2017 Annual Cyber security Report, available at: https://www.cisco.com/c/m/en_au/products/security/offers/annual-cybersecurity-report-2017.html

Clark, M., 2021. Ubiquiti is accused of covering up a 'catastrophic' data breach — and it's not denying it. The Verge. 31 March. Available at: https://www.theverge.com/2021/3/31/22360409/ubiquiti-networking-data-breach-response-whistleblower-cybersecurity-incident

CNIL, 2019. SAN-2019-001. Available at: https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf

Coffee, J.C., 2001. The Rise of Dispersed Ownership: The Roles of Law and the State in the Separation of Ownership and Control. *Yale Law Journal*, 111(1), pp.1-82.

Coyne, C.J. and Leeson, P.T., 2005. Who's to Protect Cyberspace? *Journal of Law, Economics & Policy*, 1(2), pp.473-495.

Croft, J., 2020. Hotel group Marriott faces London lawsuit over huge data breach. Financial Times. 19 August. Available at: https://www.ft.com/content/d6202d00-a173-4b15-b68a-46764934c76b

de Bruijn, H. and Janssen, M., 2017. Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, 34(1), pp.1-7.

Division of Corporation Finance, Securities and Exchange Commission, CF Disclosure Guidance: Topic No. 2 Cybersecurity Available at: https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

Dowty, M., 2017. Life Is Short. Go to Court: Establishing Article III Standing in Data Breach Cases. *S. Cal. L. Rev.*, 90, pp.683-718.

ENISA Cybersecurity Cultures in Organizations report, available at: https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations

ENISA Threat Landscape Report 2020, available at https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends

European Commission Recommendation 2013/396/EU. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013H0396&from=EN

Fama, E.F., 1970. Efficient Capital Markets: A Review of Theory and Empirical Work. *The Journal of Finance*, 25(2), pp.383-417.

Ferraro, M.F., 2013. Groundbreaking or Broken; An Analysis of SEC Cybersecurity Disclosure Guidance, Its Effectiveness, and Implications. *Alb. L. Rev.*, 77, pp.297-347.

Frimpong, B. and Chen, L., 2021. The Effects of Data Breaches on Public Companies: A Mirage or Reality? Advances in Intelligent Systems and Computing. Available at: https://link.springer.com/content/pdf/10.1007%2F978-3-030-73100-7_49.pdf

Garfinkel, S.L., 2012. The Cybersecurity Risk. Communications of the ACM, 55(6), pp.29-32.

Garg, A., Curtis, J. and Halper, H., 2003. Quantifying the financial impact of IT security breaches. *Information Management & Computer Security*, 11(2/3), pp. 74-83.

Gatzlaff, K.M. and McCullough, K.A., 2010. The Effect of Data Breaches on Shareholder Wealth. *Risk Management and Insurance Review*, 13(1), pp.61-83.

Gordon, L.A., Loeb, M.P. and Zhou, L., 2011. The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security*, 19(1), pp.33-56.

Harknett, R.J. and Stever, J.A., 2009. The cybersecurity triad: Government, private sector partners, and the engaged cybersecurity citizen. *Journal of Homeland Security and Emergency Management*, 6(1).

Hartzog, W. and Richards, N., 2020. Privacy's constitutional moment and the limits of data protection. *Boston College Law Review*, *61(5)*, pp.1687-1761.

Hayes, P., 2020. Equifax's $149 Million Data Breach Settlement OK'd. Bloomberg Law. 27 February. Available at: https://news.bloomberglaw.com/securities-law/equifaxs-149-million-data-breach-securities-settlement-gets-ok

Helman, L., 2019. Pay For (Privacy) Performance: Holding Social Network Executives Accountable for Breaches in Data Privacy Protection. *Brooklyn Law Review*, *84*(2), pp.523-569.

Hermalin, B.E. and M.S. Weisbach, 2017. The Study of Corporate Governance. In: Hermalin, B.E. and M.S. Weisbach (eds.) *The Handbook of the Economics of Corporate Governance - Volume 1*, Elsevier: Amsterdam, pp.1-15.

Hermalin, B.E., 2017. Aspects of the Economics of Organization with Application to Corporate Governance. In: Hermalin, B.E. and M.S. Weisbach (eds.) *The Handbook of the Economics of Corporate Governance - Volume 1*, Elsevier: Amsterdam, pp.17-91.

Hern, A, WannaCry, Petya, NotPetya: how ransomware hit the big time in 2017, 30 December 2017, The Guardian, available at: https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware

Hooker, M. and Pill, J., 2016. You've Been Hacked, and Now You're being Sued: The Developing World of Cybersecurity Litigation. (August), 90 *Florida Bar Journal* 30.

Hopt, K. J., 2013. Conflict of Interest, Secrecy and Insider Information of Directors, A Comparative Analysis. *European Company and Financial Law Review*, 10(2), 167-193.

Hovav, A. and D'Arcy, J., 2003. The impact of denial-of-service attack announcements on the market value of firms. *Risk Management and Insurance Review*, *6*(2), pp.97-121.

IBM 2017 – X-Force Threat Intelligence Index, available via https://www.ibm.com/security/data-breach/threat-intelligence; Symantec – 2017 – Internet Security Threat Report; Verizon – 2016 – Data Breach Investigations Report

In re Equifax Inc. Sec. Litig., 357 F. Supp. 3d 1189, 1223 (N.D. Ga. 2019).

Jang, W. and Newman, A.L., 2021. Enforcing European Privacy Regulations from Below: Transnational Fire Alarms and the General Data Protection Regulation. *JCMS: Journal of Common Market Studies*, (forthcoming).

Jensen, M.C. and W.H. Meckling, 1976. Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, 3(4), pp.305-360.

Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., and Stulz, R. M., 2018. What is the Impact of Successful Cyberattacks on Target Firms? NBER Working Paper No. 24409.

Kaplan, S. and Garrick, B.J., 1981. On the quantitative definition of risk. *Risk Analysis*, 1(1), pp.11-27.

Kaspersky Lab (2018). From data boom to data doom - The risks and rewards of protecting personal data. Available at: https://go.kaspersky.com/rs/802-IJN-240/images/Kaspersky_Lab_Business%20in%20a%20data%20boom.pdf

Kasperson, R.E., Renn, O., Slovic, P., Brown, H.S., Emel, J., Goble, R., Kasperson, J.X. and Ratick, S., 1988. The social amplification of risk: A conceptual framework. *Risk Analysis*, 8(2), pp.177-187

Klaus, T. and Elzweig, B., 2020. The impact of data breaches on corporations and the status of potential regulation and litigation. *Law and Financial Markets Review*, *14*(4), pp.255-260.

Klemash, S.W., Smith, J.C., and Seets, C., 2020. What Companies are Disclosing About Cybersecurity Risk and Oversight. Harvard Law School Forum on Corporate Governance. 25 August. Available at: https://corpgov.law.harvard.edu/2020/08/25/what-companies-are-disclosing-about-cybersecurity-risk-and-oversight/

Kostopoulos, G.K., 2017. Cyberspace and Cybersecurity, 2nd Edition. Taylor & Francis: New York.

Leggett, T., 2021. Amazon hit with $886m fine for alleged data law breach. BBC News. 30 July. Available at: https://www.bbc.com/news/business-58024116

Lehuedé, H., 2019. Corporate governance and data protection in Latin America and the Caribbean. Production Development series, No. 223 (LC/TS.2019/38), Santiago, Economic Commission for Latin America and the Caribbean (ECLAC).

Leukfeldt, E.R., 2014. Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization. *Cyberpsychology, Behavior, and Social Networking*, 17(8), pp.551-555.

Li, H., No, W.G. and Wang, T., 2018. SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems*, 30, pp.40-55.

MacCarthy, M. and Propp, K., 2021. Machines Learn That Brussels Writes the Rules: The EU's New AI Regulation. Brookings. 4 May. Available at: https://www.brookings.edu/blog/techtank/2021/05/04/machines-learn-that-brussels-writes-the-rules-the-eus-new-ai-regulation/

Marcogliese, P. and Mukhi R., 2018. Untangling the Tangled Web of Cybersecurity Disclosure Requirements: A Practical Guide. 17 June. Available at: https://corpgov.law.harvard.edu/2018/06/17/untangling-the-tangled-web-of-cybersecurity-disclosure-requirements-a-practical-guide/

Marcus, D.J., 2018. The Data Breach Dilemma: Proactive Solutions for Protecting Consumers' Personal Information. *Duke LJ*, *68*, pp.555-593.

Merken, S., 2021. Judge tosses lawsuit over Marriott's 2020 data breach. Reuters. 4 March. Available at: https://www.reuters.com/article/dataprivacy-marriott-idUSL2N2L21IQ

Moore, T. and Anderson, R., 2012. Internet Security. In: Peitz, M. and J. Waldfogel (eds.) *The Oxford Handbook of the Digital Economy*, Oxford University Press: Oxford, pp.572-599.

Mulligan, D.K. and Schneider, F.B., 2011. Doctrine for Cybersecurity. *Daedalus*, 140(4), pp.70-92.

Multistakeholder Group, 2020. Contribution from the Multistakeholder Expert Group to the Commission 2020 Evaluation of the General Data Protection Regulation. Brussels, 17 June.

NIST 2020. Privacy Framework: A Tool For Improving Privacy Through Enterprise Risk Management. 16 January. Available at: https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf

Palmer, D., 2018. Ransomware: Not dead, just getting a lot sneakier. ZDNet. 3 July. Available at: https://www.zdnet.com/article/ransomware-not-dead-just-getting-a-lot-sneakier/

Park, S., 2019. Why information security law has been ineffective in addressing security vulnerabilities: Evidence from California data breach notifications and relevant court and government records. *International Review of Law and Economics*, 58, pp.132-145.

Pietsch, B., 2019. Factbox: Biggest U.S. Data Breach Settlements before Equifax. Reuters. 22 July. Available at: https://www.reuters.com/article/us-equifax-cyber-settlement-factbox-idUSKCN1UH22P

Ponciano, J., 2021. Amazon Stock Loses $130 Billion In Market Value After $885 Million Fine And Disappointing Earnings Report. Forbes. 30 July. Available at: https://www-forbes-com.cdn.ampproject.org/c/s/www.forbes.com/sites/jonathanponciano/2021/07/30/amazon-stock-loses-130-billion-in-market-value-after-885-million-fine-and-dismal-earnings-report/amp/

Ponemon Institute, 2017. The Impact of Data Breaches on Reputation and Share Value. Available at: www.centrify.com/media/4772757/ponemon_data_breach_impact_study_uk.pdf

Ponemon Institute and IBM Security, 2017. Cost of Data Breach Study - Global Overview. Available at: https://www.securityupdate.net/SU/IBMSecurity/IBM-Security-Cost-of-Data-Breach-Study.pdf

Ralston, P.A., Graham, J.H. and Hieb, J.L., 2007. Cyber security risk assessment for SCADA and DCS networks. ISA transactions, 46(4), pp.583-594.

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)

Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (market abuse regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC

Reijmer, T. and Spruit, M.R., 2014. Cybersecurity in the news: A grounded theory approach to better understand its emerging prominence. Technical Report Series, (UU-CS-2014-006).

SANS Institute, 2017. Threat Landscape Survey: Users on the Front Line, Whitepaper, available at: https://www.sans.org/reading-room/whitepapers/threats/2017-threat-landscape-survey-users-front-line-37910

Satter, R., Bing, B, Menn, J., 2020. Hackers used SolarWinds' dominance against it in sprawling spy campaign. Reuters. 16 December. Available at: https://www.reuters.com/article/global-cyber-solarwinds/hackers-used-solarwinds-dominance-against-it-in-sprawling-spy-campaign-idUSKBN28Q07P

Scmagazine, 2021. SolarWinds lawsuits merge as stockholders begin documenting financial losses. 12 March. Available at: https://www.scmagazine.com/news/breach/solarwinds-lawsuits-merge-as-stockholders-begin-documenting-financial-losses

Securities and Exchange Commission, 17 CFR Parts 229 and 249, [Release Nos. 33-10459; 34-82746] Commission Statement and Guidance on Public Company Cybersecurity Disclosures. Available at: https://www.sec.gov/rules/interp/2018/33-10459.pdf

Securities and Exchange Commission, 17 CFR Parts 229 and 249, [Release Nos. 33-10459; 34-82746] Commission Statement and Guidance on Public Company Cybersecurity Disclosures. Available at: https://www.sec.gov/rules/interp/2018/33-10459.pdf

Skedsvold, M.C., 2018. A Duty to Safeguard: Data Breach Litigation Through a Quasi-Bailment Lens. *J. Intell. Prop. L.*, *25*, pp.201-226.

Solicitors' claim, 2020. MR STEPHEN WEAVER & OTHERS Claimants against BRITISH AIRWAYS PLC Defendant. Available at: https://files.lbr.cloud/public/2020-06/BA%20particulars%20of%20claim.pdf?BrAt.nnYUI75cuvkZ2oOSF8d7fM9HWLc

Southwell, A. H., 2017. Gibson Dunn Reviews U.S. Cybersecurity and Data Privacy. Columbia Law School Blue Sky Blog. Available at: http://clsbluesky.law.columbia.edu/2017/02/03/gibson-dunnreviews-u-s-cybersecurity-and-data-privacy/

Stubbs, M., 2020. Equifax Agrees to $149 Million Settlement for Infamous 2017 Data Breach. Expert Institute. 25 June. Available at: https://www.expertinstitute.com/resources/insights/equifax-agrees-to-149-million-settlement-for-infamous-2017-data-breach/

Tidy, J., 2020. British Airways fined £20m over data breach. BBC News. 16 October. Available at: https://www.bbc.com/news/technology-54568784

Tidy, J., 2020. Marriott Hotels fined £18.4m for data breach that hit millions. BBC News. 30 October. Available at: https://www.bbc.com/news/technology-54748843

Trautman, L.J. and Altenbaumer-Price, K., 2010. The board's responsibility for information technology governance. *J. Marshall J. Computer & Info. L.*, *28*, pp.313-342.

Trope, R.L. and Hughes, S.J., 2011. The SEC Staff's Cybersecurity Disclosure Guidance: Will It Help Investors or Cyber-Thieves More. Bus. L. Today, pp.1.

Uberti, D., 2021. GOP Bill Attempts to Inject Life Into Stalled Internet Privacy Talks. Wall Street Journal. 28 July. Available at: https://www.wsj.com/articles/gop-bill-attempts-to-inject-life-into-stalled-internet-privacy-talks-11627464601

van den Berg, B., 2016. Coping with information underload. In: Hildebrandt, M. and B. van den Berg (eds.) *Information, Freedom and Property*, Routledge: Abingdon UK, pp.173-199.

Wolff-Mann, E., 2019. Equifax used 'admin' as username and password for sensitive data: lawsuit. Yahoo Finance. 18 October. Available at: https://finance.yahoo.com/news/equifax-password-username-admin-lawsuit-201118316.html

World Economic Forum, 2018. Global Risks Report, available at: http://reports.weforum.org/global-risks-2018/global-risks-landscape-2018/#landscape