# Regulating cybersecurity : what civil liability in case of cyber-attacks ?

de Werra, Jacques; Studer, Evelyne

EVELYNE STUDER
JACQUES DE WERRA

# REGULATING CYBERSECURITY

## What civil liability in case of cyber-attacks? [1]

**In spite of the growing risks posed by cyber-attacks, the legal fallout and, specifically, the civil liability resulting from such attacks is still unclear and raises complex legal issues namely because of the diversity of potentially applicable liability regimes (which include personal data and product liability regulations). It may thus be that legislative action on this issue will be warranted at some point in the future.**

### 1. INTRODUCTION

The issues of cybersecurity and cyber-attacks have progressively reached the top of the agenda of companies and governments alike due in no small part to the recent global waves of severe cyber-attacks. Cyber-attacks are no longer potential futuristic risks or threats but very real events that affect both businesses and individuals as a result of our society's increasing dependency on information and communications technologies [2]. Particularly as regards businesses, any one of them could be targeted: the former CEO of *Cisco Systems, John Chambers,* famously stated in this respect that "[t]here are only two types of companies: Those that have been hacked and those that don't know they have been hacked" [3].

Even though no unique definitions of the terms "cybersecurity" and "cyber-attacks" have been adopted at the global level [4], we shall consider here that "cybersecurity" covers "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user's assets" [5] and that "cyber-attack" refers to the intentional disruption of an information system's confidentiality, integrity, or availability (also known as the CIA triad in the information security industry [6]) [7].

In the rising tide of cyber-attacks, it is crucial to identify what civil liability-related risks are associated with such attacks under existing law [8]. Further, at the policy level, it is important to explore what regimes of liability can create security-enhancing incentives without causing adverse side effects, such as the stifling of innovation.

Liability is a central element of the cybersecurity/cyber-attacks debate. The reason, as computer security expert *Bruce Schneier* succinctly put it, is that "liability changes everything" [9]. The power to enhance cybersecurity and to mitigate cyber-attacks lies today in the hands of the private sector [10]. Since developing and maintaining a robust cybersecurity infrastructure entails costs, sufficient incentive – created namely through legal liability – must exist in order to motivate the industry to work towards a high level of cybersecurity [11]. As Schneier puts it, "[t]he only way to convince vendors to actually fix the problem [of insufficient cybersecurity] is to make it in their financial interest to do so" [12]. Failing a sufficient incentive for voluntarily actions, companies will undertake a cost-benefit analysis that might well show that the cost of designing and implementing robust cybersecurity measures against hostile cyber-intrusions and of fixing vulnerabilities/design flaws in the first place is ultimately higher than the loss that may result from such cyber-intrusions. However, much as incentives to make the IT infrastructure more resilient to hostile cyber-intrusions are necessary, they are currently lacking [13].

Businesses in various industries have generally resisted the imposition of legal cybersecurity responsibility based on the (fair) argument that there is no such thing as perfect cybersecurity, particularly when it comes to software, in view of the notorious unfeasibility of developing absolutely secure code [14]. Businesses also claim that the introduction of stringent liability risks impeding innovation and therefore paralyzing the industry [15]. The end result is that cybersecurity in the private sector is in a poor state, and that public security

EVELYNE STUDER,
RESEARCH AND TEACHING ASSISTANT,
SCHOOL OF LAW,
UNIVERSITY OF GENEVA,
GENEVA

JACQUES DE WERRA,
PROFESSOR,
SCHOOL OF LAW,
UNIVERSITY OF GENEVA,
VICE-RECTOR OF THE UNIVERSITY, GENEVA

and the society as a whole are bearing the cost of adverse cyber events [16]. Consequently, a growing number of experts argue that liability for damages caused by hostile cyber-intrusions which could have been reasonably preventable should be introduced and assigned to private industry stakeholders since vulnerabilities, defects or insufficient cybersecurity in their infrastructure, software, or products created the opportunities for the intrusion in the first place. Yet, construing such a legal and policy framework is no easy feat and has until now eluded lawmakers.

*"Businesses in various industries have generally resisted the imposition of legal cybersecurity responsibility based on the (fair) argument that there is no such thing as perfect cybersecurity."*

Under existing law, the legal exposure of a business targeted by a cyber-attack is difficult to assess. This is largely due to the many unresolved questions that the allocation of liability poses in such a case. In particular, it poses the question of due care and the related threshold question as to what level of cybersecurity might be deemed reasonable and appropriate so that, notwithstanding an attack, no liability can be assigned to the victim. Adding to the complexity of this question is the fact that any regulatory standard of "reasonable cybersecurity measures" will likely vary depending on the context and the nature of the affected data.

Further, the allocation of liability raises the question as to whether liability could be imposed in situations of potential secondary liability [17]. For instance, in a case where a cyber-attack on a corporation causes harm to third parties (which does not constitute a personal data breach, see below subpart 2.2.2), could liability to the third parties be imposed on the target of the attack for failing to prevent or protect against the malicious attack, thereby putting it in a "victim-defendant" position [18]? If so, what act or omission would be deemed a "legally relevant contribution", sufficient to establish secondary liability [19]?

Besides, questions arise in situations that involve a chain of parties that may have contributed, albeit unintentionally, to the cyber-attack. Take the example of the recent *WannaCry* ransomware that spread throughout the Internet and affected Windows-based computer systems that were running on outdated software [20]. The attack caused disruptions at countless places, including hospitals, businesses, and universities [21]. A stream of (potential) liability flows from the attack with various parties to blame for it. Such parties include not only the programmers of the malware and the hackers' group, but also potentially the users who failed to install the Windows security patch as the vulnerability was discovered and the patch announced, and Microsoft, as the software vendor, which wrote the insecure code in the first place [22]. It is unclear how liability will be allocated (if at all) between such parties [23]. In particular users (including businesses) that failed to install the Windows security patch could potentially face legal actions (not limited to civil actions) for lax cybersecurity or for the negligent failure to deliver services following the attack [24]. As a side note, digressing from the issue of civil liability, it is noteworthy that some predict that businesses that failed to update their software could face scrutiny from the *U.S. Federal Trade Commission (FTC)* for misrepresenting their data privacy measures [25].

The difficulty of allocating liability when several parties are involved also arises when a multitude of actors are involved in a particular process or environment. This is namely the case in the *Internet of Things (IoT)* context, where a complex chain of interconnected products stem from different suppliers, such as software vendors or sensor manufacturers [26]. For instance, if a smart phone from manufacturer A that runs IoT software created by third party software developer B were the target of a security hack made possible by a software vulnerability in the software of developer B, it is unclear who would be held liable for any resulting damage.

In view of the above, the aim of this article is to identify selected issues relating to the problem of civil liability exposure in the event of a cyber-attack (see below II) [27] and to lay out a number of policy considerations regarding such issues (see below 3).

## 2. CIVIL LIABILITY FOR CYBER-ATTACKS

Companies currently face a great deal of uncertainty when assessing the risk of legal liability that may arise from or following a cyber-attack. This issue is compounded by a fragmented and evolving legal landscape [28]. The following subparts will consider selected cases of civil liability [29], whereby civil liability generally falls into one of two categories: contractual liability (see below 2.1), or non-contractual (tort) liability (see below 2.2).

**2.1 Contractual liability.** In presence of a contractual relationship, such as between an Internet platform and its users, the user who suffers a damage as a result of a cyber-attack could potentially bring a contract-based action against his or her contractual partner on the basis of a contractual promise of security, contained for instance in a privacy policy [30]. This occurred for example in a US case where LinkedIn was sued by customers for having misled them about its data protection policies, falsely claiming that it offered industry-standard cybersecurity measures, when in reality its security was outdated and insufficient [31]. The suit was brought after LinkedIn suffered a data breach that led to millions of emails and password combinations to be posted online. The

*"Companies currently face a great deal of uncertainty when assessing the risk of legal liability that may arise from or following a cyber-attack."*

class was namely made up of premium LinkedIn subscribers who had reviewed LinkedIn's privacy policy and had been influenced by its representations about the level of security [32].

Under Swiss law [33], a breach of contract claim would be based on Art. 97 of the *Swiss Code of obligations (CO),* which sets forth the general conditions of contractual liability, i.e (i) a breach of contract (such as a breach of the duty to provide the promised level of cybersecurity), (ii) an actual damage, (iii) a causal link between the breach and the damage, and (iv) a fault (which is presumed). Based on this provision, the Internet platform could prima facie appear to be potentially exposed to contractual liability for damages resulting from the failure to provide the promised security, unless it can prove that it did not commit any fault (and assuming that the other conditions are met).

This scenario however raises several issues. The first one is that contractual liability under Swiss law is fault-based. While such fault is presumed – which, from the plaintiff's perspective is one of the advantages of bringing a breach of contract action – it can nonetheless not be excluded that the defendant Internet platform could demonstrate that it did not commit any fault in relation to the cyber-attack. An additional issue for the plaintiff relates to the potential difficulty of demonstrating the causal link requirement between the breach of contract and the damage purportedly suffered.

In addition, contractual liability may not apply since standard terms of service frequently do not contain any promise of security. On the contrary, vendors, and especially software vendors, typically attempt to minimize or even exclude their civil liability by inserting warranty disclaimers and limitations of liability in their terms of service [34]. Thus, terms of service typically provide that, in the event of a breach, neither party will be responsible for the other party's consequential damages and that any potential liability is limited to direct damages [35]. That said, it is questionable whether such limitations of liability would be upheld in the event of a cyber-attack, since liability limitations may be deemed null and void in the case of gross negligence (see, for Swiss law, Art. 100 CO). On this basis, it appears that the risk that a vendor might be subject to contractual liability in the event of a cyber-attack will generally be limited, provided however that the vendor was not grossly negligent in implementing and maintaining adequate cybersecurity measures.

### 2.2 Tort liability

*2.2.1 General remarks.* In the absence of a contractual relationship, courts could impose tort liability on companies for the harm that a cyber-attack causes to third parties. Any contractual disclaimers or limitations of liability (discussed under 2.1 above) would not be binding on such third parties.

Under Swiss law, tort liability is governed by Art. 41 CO and is subject to the following conditions: (i) an illicit act, (ii) an actual damage, (iii) a causal link between the illicit act and the damage, and (iv) a fault (which is not presumed). Based on case law, an illicit act under Art. 41 CO exists if the act breaches a general legal obligation, which can result from the breach of an absolute right of the victim (such as a right of personality, an intellectual property right, etc.) or from the monetary damage resulting from the breach of a specific legal provision that protects the victim against such damage ("Schutznorm") [36].

In relation to cyber-attacks, tort liability raises its fair share of issues as well. First, a plaintiff might encounter difficulties in proving the existence of an illicit act in relation to a cyber-attack in the absence of a violation of an absolute right of the victim (such as the right to the protection of personal data) and in the absence of a specific provision providing for a cause of tort liability [37]. While corporations can have a legal duty to protect the information of their customers, it is unclear what the extent of such legal duty would be vis-à-vis third parties (at times referred to as "downstream" victims), in cases where the corporation is not a custodian of specific types of data (such as personal or financial data) [38].

Tort liability can result from a wide range of different sources, including data protection rules (see below 2.2.2) and product liability rules (see below 2.2.3). Tort liability can also potentially result from a specific software liability regime for software products that could be introduced (see below 2.2.2.4). The below subparts will examine these issues from a EU law perspective, in view of their potential impact beyond the EU (including on Swiss law/Swiss-based companies).

*2.2.2 Data protection.* Companies that process [39] personal data [40], which is virtually all companies, and that fall under the extensive scope of the Regulation (EU) 2016/679, *General Data Protection Regulation (GDPR)* have until 25 May 2018 to comply with the new EU data protection legislation.

The GDPR sets forth a civil liability regime for data controllers (who determine the purpose and means of the processing of personal data) and data processors (who process personal data on the behalf of controllers) [41].

Under this regime, controllers, who bear the primary responsibility to ensure that processing activities are compliant with the GDPR, are liable for the damage caused by processing that infringes the GDPR (Art. 82 (2)). As to processors, their liability exposure is more limited since they are liable only where they have not complied with obligations specifically directed at them under the GDPR, or have acted outside of or contrary to lawful instructions from the data controller (Art. 82 (2)).

The liability exposure of controllers and processors depends on the nature of the relevant obligation (i.e. obligation or means or obligation of result). Art. 32 GDPR sets forth an obligation of means [42]. This provision is relevant for our purposes since it requires controllers and processors to implement "appropriate technical and organisational measures to ensure a level of security appropriate to the risk", taking into account in particular "the state of the art". While it is unclear what such measures concretely entail, the GDPR offers some examples of the type of security measures that might be considered "appropriate to the risk," including "the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services" (Art. 32 (1) (b)), and "a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing" (Art. 32 (1) (d)). Additionally, the assessment of the "appropri-

ate level of security" must take into account the risks caused by the relevant processing, such as in particular the risk of unlawful destruction, loss, alteration or unauthorized disclosure of, or access to personal data (Art. 32 (2)). What is more, the technical and organizational measures must be regularly reviewed and updated where necessary (Art. 24 (1)). This last element is particularly important in relation to cyber-attacks since, according to a Verizon report, 99.9 percent of all vulnerabilities exploits are perpetrated more than a year after the vulnerability was disclosed [43].

*"A recurring theme in the cybersecurity debate is that insecure software is one of the key contributors of the cyber-insecurity problem, given how deeply software is embedded in the foundation of our modern world."*

The civil liability regime for controllers is a strict liability regime [44]. Controllers can therefore not escape liability merely by proving the absence of a fault on their part. The GDPR does however contain an escape clause, based on which a controller can claim an exemption of liability if it successfully establishes that it is not "in any way" responsible for the event that gave rise to the damage (Art. 82 (3)). It is unclear what the terms "in any way" will mean in practice, particularly in relation to the obligation of means set forth at Art. 32 GDPR. However, the addition of the terms "in any way" (which were not included in the relevant provision of the Directive 95/46 (Data Protection Directive) [45] that the GDPR will replace), seems to indicate a willingness to narrow the scope of the liability exemption [46].

In light of the above, the civil liability exposure of companies that fall within the broad scope of application of the GDPR is potentially significant. In addition, it is worth noting that the GDPR explicitly provides that data subjects are entitled to have their right to bring a private claim for damages exercised by a non-for-profit body, organizations or association on their behalf (Art. 8). This means that under the new Regulation, mass-claims in the case of large-scale infringements are possible [47].

*2.2.3 Products liability.* At its core, products liability law aims at controlling the defective implementation of consumer technologies and protecting consumers from "exploding toasters and other hazards" [48].

The liability regime under the Directive on liability for defective products (85/374/CEE) (Products Liability Directive) is an example of *ex post* liability, where liability is assigned to the responsible party with the rationale that the threat of monetary damages stemming from legal actions will incentivize actors to implement the necessary measures to minimize the risk of failures or defects [49].

The Products Liability Directive sets forth a strict liability regime [50]. To the extent that a defective product causes a damage to a consumer, liability may be imposed on the producer even without negligence or fault on its part (Art. 1). Liability is however limited to the producer and cannot be imposed on to third parties. The type of recovered damages is also limited to damage caused by death or by personal injuries and to damage to, or destruction of, any item of property other than the defective product itself which is intended for and effectively used for the private use (Art. 9). The Directive places the burden of proof on the injured party as regards the damage, the defect, and the causal relationship between the two (Art. 4).

Difficulties arise in respect of the application of the Products Liability Directive in certain technological contexts [51]. Taking for instance the IoT environment, it is difficult to determine what the product liability exposure of software vendors to claims for personal injury and property damage caused to third parties could be. It is particularly unclear how the terms "defective" will be interpreted in such a context. Such interpretation is however important since, although a fault on the part of the producer is not required, the plaintiff must nevertheless prove, among other things, the defective nature of the product. According to Art. 6 of the Product Liability Directive, a product is defective "when it does not provide the safety which a person is entitled to expect, taking all circumstances into account, [...]". IoT devices are notoriously vulnerable to the possibility of cyber-intrusions. Thus, the question that arises is what level of security IoT users are generally "entitled to expect" to protect them against hacking [52]. Such expectation of safety may further vary depending on the specific market in which the IoT device operates [53]. The question also arises as to whether the notion of "defect" as provided under the Products Liability Directive should be replaced by that of "lack of safety/security".

*"At its core, products liability law aims at controlling the defective implementation of consumer technologies and protecting consumers from 'exploding toasters and other hazards'."*

In any event, the practical consequences of the application or non-application of product liability rules should not be underestimated, also from a Swiss perspective, knowing that the Swiss Product Liability Act (PLA) mirrors to a large extent the provisions of the Products Liability Directive. What is clear is that the risk of cyber(in)security leading to potential physical harm, especially in the IoT context, is a very real concern [54]. One only needs to think of intelligent aircraft, smart cars or smart medical devices being hacked to see that IoT powered things do indeed have the potential to cause "death or personal injuries".

*2.2.4 Specific liability regime for software products?* A recurring theme in the cybersecurity debate is that insecure software is

one of the key contributors to the cyber-insecurity problem, given how deeply software is embedded in the foundation of our modern world [55].

Software developers control to a large extent the security of the systems that they are developing. However, generally, software methodologies do not focus on the quality or security of the software product but rather on functionality and time-to-market [56]. Often, software manufacturers knowingly rush to market with products that still have vulnerabilities and design defects, eager to reduce time to market, with the approach "ship now, patch later" [57]; [58].

Under current law, it appears that software vendors are effectively insulated from liability where such liability arises in a situation that falls outside the scope of product liability regulations [59]. This is the result of the longstanding efforts of the software industry to resist binding formulations of the due diligence that developers are required to exercise as well as avoid ex post liability for vulnerabilities in its products by resisting external regulation on the quality, safety or security of its products [60]. In the US for instance, Congress even amended the *Computer Fraud and Abuse Act (CFAA)* in 2001 to make clear that civil liability for defective programming did not attach to software manufacturers [61].

There have been numerous calls worldwide to hold software vendors liable for the damage resulting from the exploitation of vulnerabilities in their products, such as the damage caused by a cyber-attack [62]. Particularly the inherently insecure IoT ecosystem has rekindled the discussion about "ending the software industry's long-standing exemption from legal liability for defects in its products" [63].

However, there have also been voices against the imposition of software manufacturer liability, which contend that imposing such liability would demonstrate "a lack of strategic foresight". The argument here is that liability enforced by end-users would not be a strategic approach since, even assuming that the substantive law would successfully hold software manufacturers liable, end-users may not be willing to make use of this option as their potential recovery would not counterbalance the burden of judicial proceedings [64].

It is noteworthy that such users may even themselves be the target of enforcement. For instance, the US FTC, under its limited mandate to take action against "unfair [or deceptive] acts or practices", initiated action against software users whose systems were breached and where third party confidential information was disclosed [65]. The FTC's efforts were mostly directed at non-financial firms which suffered massive breaches of personal data [66].

## 3. SELECTED POLICY CONSIDERATIONS

**3.1 What duty of care?** The different potential sources of tort liability for cyber-attacks raise the fundamental question of the duty and standard of care that should apply. Should there be an obligation of care "not to create situations of risk that might foreseeably be exploited by criminals to attack others, [since this is arguably] the same as that applied in the physical world in the case of keys left in a vehicle" [67]?

The digital environment creates a very high level of interconnection between people [68]. Arguably, such interconnection makes it equitable to require participants to "look out for each other and [...] adopt a more expansive conception of duty that might otherwise have been adopted" [69]. In the same vein, in the digital context "[t]he number of parties to which one owes a duty of care is greater" [70].

Another element to be taken into account is the constant evolution of the duty of care caused by the dynamic nature of the standard of care. With regard for instance to software products, this raises the issue of updates and patches which may not necessarily be available. Due to resource or technological constraints, most IoT devices are designed without the ability to accommodate software or firmware updates. As a result, vulnerability patching is difficult, if not impossible [71]. Consequently, if a duty of care that specifically includes patching is introduced, it could put organizations in an impossible position since, depending on the layers of complexity of the software, it may be impossible to upgrade or patch systems [72].

*"Obviously, purely national frameworks are unlikely to be effective as regards the imposition of civil liability in the event of a cyber-attack, given that such attacks are not necessarily restricted to any national territory."*

**3.2 Regulatory options: liability – and what else?** A possible alternative to black letter law is soft law and auto-regulation with industry partners. It may be worth thinking about how risk management could be an incentive for manufacturers to implement more robust security. Accepting that security failures are inevitable, an alternative approach could be to encourage more responsible software development by vendors by requiring software vendors to demonstrate that their software development methodologies includes adequate testing and robust responses to adverse cyber events [73].

**3.3 Need for a collaborative international framework.** Obviously, purely national frameworks are unlikely to be effective as regards the imposition of civil liability in the event of a cyber-attack, given that such attacks are not necessarily restricted to any national territory. Also, one state's laws on civil liability can and will affect citizens of another state due to the potential cross-border nature of a cyber-attack. Therefore, a collaborative international framework should be implemented. In addition, it could make sense to consider the adoption of transversal liability regimes in respect of cybersecurity risks. Finally, the framework should remain flexible and evolving so as to keep up with the speed-light developments of the technological environment in which cyber-attacks occur.

**3.4 Striking the right balance.** While there are many reasons to resist making policy recommendations aimed at cybersecurity generally [74], the following will nonetheless lay out a few considerations in relation to the legal liability framework.

Fundamentally, questions that arise deal with the types of liability regimes than can create security-enhancing incentives and with the means that can motivate the industry to enhance cybersecurity without causing adverse effects. Voluntary security practices aimed at creating enhanced cybersecurity are unlikely to be widely adopted failing sufficient economic incentives [75]. The question thus is whether the law should push towards the private-sector internalizing security costs by imposing liability ("Haftung als Security-Anreiz?" [76])?

Based on the "least cost avoider" principle, there are valid arguments that corporations should be pressured through liability to improve their infrastructure and products and manage the risk of a cyber-breach since, compared to end-users, they can do so at a lesser cost and also because they have the best information about their products [77]. In relation to cybersecurity, liability is, at least in theory, game-changing in that it arguably makes "those in the best position to fix the problem [...] actually responsible for the problem" [78]. The cost of liability can then be spread over the entire user base [79].

This approach was mentioned in the EU Commission's 2017 communication on "Building A European Data Economy", in which the EU Commission considered exploring a "risk-generating or risk-management" approach, following which "liability could be assigned to the market players generating a major risk for others or to those market players which are best placed to minimise or avoid the realisation of such risk" [80]. This position was also widely echoed in several states, including in Germany, where the suggestion was namely made that Germany should introduce liability for IT products to increase the industry's accountability [81].

However, introducing liability could create significant negative side effects as well. The main negative effect of too stringent legislation dealing specifically with liability in the field of technological innovation is to stifle innovation [82]. Indeed, "[i]f each new line of code creates a new exposure to a lawsuit, it is inevitable that fewer lines of code will be written" [83]. Thus, potential defendants must also be appropriately protected from the risk of a disproportionately wide range of liabilities: "any attempt to systematically hold vendors accountable for vulnerabilities must build in realistic constraints, or risk exposing the industry to crushing liability" [84].

**Notes: 1)** This article represents the sole views of the authors. Feedback is welcome and may be sent to evelyne.studer@unige.ch/jacques.dewerra@unige.ch. **2)** For Switzerland, see e.g. the 2016 report by the Federal Council on the security policy of Switzerland, 26, https://www.newsd.admin.ch/newsd/message/attachments/ 45069.pdf. All links to websites were last accessed on 26 June 2017. **3)** John Chambers, What does the Internet of Everything mean for security?, 21 January 2015, https://www.weforum.org/agenda/2015/01/companies-fighting-cyber-crime/?utm_content=bufferbo881&utm_medium=social&utm_source=facebook.com&utm_campaign=buffer. **4)** Jeffrey F. Addicott, Enhancing Cybersecurity in the private sector by means of civil liability lawsuits – the Connie Francis effect, 51 U. Rich. L. Rev., 857–895, 2017, 875, http://lawreview.richmond.edu/files/2017/03/Addicott-513.pdf; Trey Herr/Allan Friedman, Understanding Cybersecurity – Part 1, Redefining Cybersecurity, The American Foreign Policy Council, January 2015, http://www.afpc.org/publication_listings/viewPolicyPaper/2664. See also Building an Effective European Cyber Shield Taking EU Cooperation to the Next Level, 8 May 2017, https://ec.europa.eu/epsc/publications/strategic-notes/building-effective-european-cyber-shield_en ("Yet, there remains a gap between the level of maturity of cyber threats and that of worldwide norms and definitions in the cyber context (e.g. what is an 'attack' in cyberspace?"). There isn't even an agreement on its spelling, see the report by the European Union Agency for Network and Information Security (ENISA) on "Definition of Cybersecurity, Gaps and overlaps in standardization", December 2015, 10, https://www.enisa.europa.eu/publications/definition-of-cybersecurity ("Even the correct spelling of 'Cybersecurity' is controversial and differing"). **5)** ITU Definition of cybersecurity, http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx. **6)** Axel M. Arnbak, Securing private communications: Protecting private communications security in EU law: fundamental rights, functional value chains and market incentives, Amsterdam, 2015, 30 and 155 f. **7)** Addicott (n. 4), 869. **8)** It should be noted that the focus here will be on the potential liability of the companies that are the victims of cyber-attacks, and not on the cyber-attackers who will generally bear the primary liability. **9)** Bruce Schneier, Liability changes everything, November 2003, https://www.schneier.com/essays/archives/2003/11/liability_changes_ev.html. **10)** Amitai Etzioni, Cybersecurity in the Private Sector, Issues in Science and Technology, Fall 2011, 58-62, 59, http://gwdspace.wrlc.org:8180/xmlui/bitstream/handle/1961/10590/B530-cybersecurity-private-sector.pdf?sequence=4. **11)** Etzioni (n. 10), 59. **12)** Bruce Schneier, RSA 2012: Are Software Liability Laws Needed?, 1 March 2012, https://www.schneier.com/news/archives/2012/03/rsa_2012_are_softwar.html. See also the article published in the Economist, Incentives need to change for firms to take cyber-security more seriously, 20 December 2016, http://www.economist.com/news/leaders/21712138-software-developers-and-computer-makers-do-not-necessarily-suffer-when-their-products-go. **13)** According to the director of the Center for Applied Cybersecurity Research at Indiana University and a member of government-appointed information-security advisory boards, Fred H. Cate, cybersecurity is desperately in need of better incentives, see Etzioni (n. 10), 59. **14)** Jay Pil Choi/Chaim Fershtman/Neil Gandal, Network Security: Vulnerabilities and Disclosure Policy, 58 Journal of Industrial Economy, 2010, 869. **15)** David Rice, Geekonomics: The Real Cost of Insecure Software, 2007. **16)** Etzioni (n. 10), 59. Bearing in mind, however, that there is some contention about the real cost of cyber-attacks and cyber-incidents, see e.g. the 2016 Ponemon study on "Cost of Cyber Crime Study & the Risk of Business Innovation", http://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20 FINAL%203.pdf. **17)** Julian Totzek-Hallhuber, Gehackt – wer haftet?, 30 March 2017, https://www.computerwoche.de/a/gehackt-wer-haftet,3330421. **18)** On this issue, see in particular Adrien Alberini, Le paradoxe des cyberattaques: la responsabilité des victimes, 21 May 2017, https://www.letemps.ch/opinions/2017/05/21/paradoxe-cyberattaques-responsabilite-victimes. See also Julian Totzek-Hallhuber, Gehackt – wer haftet?, 30 March 2017, https://www.computerwoche.de/a/gehackt-wer-haf tet,3330421. **19)** On the general principles of secondary liability in the fields of intellectual property, unfair competition, data protection and rights of personality, see e.g. Cyrill Rigamonti, Secondary Liability of Internet Service Providers in Switzerland, in: Swiss Reports Presented at the XIX$^{th}$ International Congress of Comparative Law, http://www.iwr.unibe.ch/ueber_uns/prof_dr_cyrill_p_rigamonti/e163247/e163141/files163157/Rigamonti_ISP-Liability.pdf. **20)** Bruce Schneier, WannaCry and Vulnerabilities, 2 June 2017, https://www.schneier.com/blog/archives/2017/06/wannacry_and_vu.html. **21)** Bruce Schneier, WannaCry and Vulnerabilities, 2 June 2017, https://www.schneier.com/blog/archives/2017/06/wannacry_and_vu.html. **22)** Bruce Schneier, WannaCry and Vulnerabilities, 2 June 2017, https://www.schneier.com/blog/archives/2017/06/wannacry_and_vu.html. **23)** Rodrigo F. Guerra, "WannaCry"?... In a liability world, 15 May 2017, https:// www.linkedin.com/pulse/wannacry-liability-world rodrigo-f-guerra. **24)** Jan Wolfe, Cyber-attack could spark lawsuits

but not against Microsoft, 16 May 2017, http://www.reuters.com/article/us-cyber-attack-liability-idUSKCN18B2SE. **25)** Jan Wolfe, Cyber-attack could spark lawsuits but not against Microsoft, 16 May 2017, http://www.reuters.com/article/us-cyber-attack-liability-idUSKCN18B2SE. **26)** Mason Hayes & Curran, 19 May 2016, Untangling the Web of Liability in the Internet of Things, https://www.mhc.ie/latest/blog/untangling-the-web-of-liability-in-the-internet-of-things. **27)** In view of space constraints, this article will not explore the issue of the personal civil liability of the management (directors/officers) of companies for cyber-attacks. On this issue, see Richik Sarka, 4 Cybersecurity Considerations To Minimize D&O Exposure, 5 June 2017, https://www.law360.com/articles/928900/4-cybersecurity-considerations-to-minimize-d-o-exposure. This article will not analyze either the legal issues relating to the insurances for cyber-risks/against cyber-attacks. On this issue, see Brendan Hogan, Why your company needs cyberinsurance, The Privacy Advisor, 28 February 2017, https://iapp.org/news/a/why-your-company-needs-cyber-insurance/. **28)** For a general presentation about IT-security and law, see Rolf Weber/Annette Willi, IT-Sicherheit und Recht, Grundlagen eines integrativen Gestaltungskonzepts, Zurich 2006. **29)** In view of space constraints, this article will focus on the civil liability arising in connection with the actual cyber-breach/cyber-attack, and not on the potential liability resulting from the company's response to the breach/attack, which would particularly include issues of breach notification obligations. Suffice it to note that such requirements may be triggered in the event of a cyber-attack, depending on the facts and nature of the data (e.g. personal data), and may be based on contract or on a regulation. **30)** Wayne M. Alder, Data Breaches: Statutory and Civil Liability, and How to Prevent and Defend A Claim, http://www.becker-poliakoff.com/data-breaches-prevent-and-defend-a-claim. **31)** Igor Kossov, LinkedIn Strikes $1.25M Settlement In Data Breach Action, 18 August 2014, https://www.law360.com/articles/568135/linkedin-strikes-1-25m-settlement-in-data-breach-action. **32)** Igor Kossov, LinkedIn Strikes $1.25M Settlement In Data Breach Action, 18 August 2014, https://www.law360.com/articles/568135/linkedin-strikes-1-25m-settlement-in-data-breach-action. **33)** Reference is made to Swiss law here, knowing that other laws will in general terms lead to a similar analysis. **34)** This article will not discuss the issue as to whether terms of service might be deemed invalid or unenforceable between a business and an individual consumer on the basis of consumer protection legislation. **35)** Scott Nonaka/Kevin Rubino, Contracting in the Cloud: Who Pays for a Data Breach?, 18 October 2016, https://www.bna.com/contracting-cloud- paysn57982078761/. **36)** BGE 141 III 527 para. 3.2. **37)** Which can result from criminal law (such as computer fraud acts). **38)** National Research Council, Critical Information Infrastructure Protection and the Law: An Overview of Key Issues, 2003, 45-46, https://www.nap.edu/read/10685/chapter/5#45. **39)** Processing is defined as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction" (Art. 4 (2) GDPR). **40)** Personal data is defined as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" (Art. 4 (1) GDPR). **41)** As mentioned in footnote 29, this article will not discuss the issue of breach notification obligations. It should nonetheless be noted that the GDPR contains a new breach notification regime and that sanctions in case of non-compliance are potentially severe. **42)** Brendan Van Alsenoy, Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation, 2016, 284, https://www.jipitec.eu/issues/jipitec-7-3-2016/4506/van_alsenoy_liability_under_eu_data_protection_law_jiptec_7_3_2016_271.pdf. **43)** Verizon 2015 Data Breach Investigations Report, http://www.verizonenterprise.com/DBIR/. **44)** Van Alsenoy (n. 42), 274. **45)** Under the Data Protection Directive the exemption can be claimed by a controller who can prove "that he is not responsible for the event giving rise to the damage". **46)** Van Alsenoy (n. 42), 283. **47)** Loyens & Loeff, GDPR – Sanctions for non-compliance, 8 June 2017, https://www.loyensloeff.com/en-us/news-events/news/gdpr-sanctions-for-non-compliance. **48)** Susan Brenner, Law in an Era of Pervasive Technology, 15 Widener L.J. 667, 2006, 764. **49)** On ex post liability, see Tyler Moore, Introducing the Economics of Cybersecurity: Principles and Policy Options, in: Proceedings of a Workshop on Deterring Cyber-attacks: Informing Strategic and Developing Options for US policy, National Academy of Sciences, 10, https://cs.brown.edu/courses/csci1800/sources/lec27/Moore.pdf. **50)** European Commission, Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions, "Building A European Data Economy", 10 January 2017, 4.1, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017DC0009&from=FR#footnoteref11. **51)** EU Commission Communication "Building A European Data Economy" (n. 50), 4.1. **52)** Jamie Cartwright, Product liability and the internet of things, 21 April 2017, http://www.lexology.com/library/detail.aspx?g=5cbef66b-1981-4445-9cad-6c744861543e. **53)** Jamie Cartwright, Product liability and the internet of things, 21 April 2017, http://www.lexology.com/library/detail.aspx?g=5cbef66b-1981-4a45-9cad-6c744861543e. **54)** See however Christian Laux/Jan Widmer, Produkthaftung für Open-Source Software? in: B. Lutterbeck/M. Bärwolff/R. A. Gehring (eds): Open Source Jahrbuch 2007 – Zwischen freier Software und Gesellschaftsmodell, Berlin 2007, 237 (holding that "[d]ie praktischen Konsequenzen aus der Anwendbarkeit des Produkthaftungsrechts werden sich jedoch in Grenzen halten, da Software meistens 'nur' Datenverluste verursacht, nicht aber Körperschäden"). **55)** Jennifer A. Chandler, Security in Cyberspace: Combatting Distributed Denial of Service Attacks, University of Ottawa Law & Technology Journal, Vol. 1, p. 231, 2003–2004, 248, http://uoltj.ca/articles/vol1.1-2/2003-2004.1.1-2.uoltj.Chandler.231-261.pdf. **56)** Liis Vihul, The Liability of Software Manufacturers for Defective Products, The Tallinn Papers No. 2, 2014, 13 https://ccdcoe.org/publications/TP_Vol1No2_Vihul.pdf. **57)** Karen Mercedes Goertzel, Legal Liability for Bad Software, CrossTalk—September/October 2016, 23, http://static1.1.sqspcdn.com/static/f/702523/27213494/1472233517737/201609-Goertzel.pdf?token=fkKNqhSQonDHOnKscqICCosk5b4%3D. **58)** Kevin R. Pinkney, Putting Blame Where Blame Is Due: Software Manufacturer and Customer Liability for Security-Related Software Failure, 13 Alb. L.J. Sci. & Tech. 43, 2002, 46. **59)** Jay Keysan/Carol Mullins Hayes, Bugs in the Market: Creating a Legitimate, Transparent, and Vendor-Focused Market for Software Vulnerabilities, 2016, 786, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2739894. **60)** Moore (n. 49), 10. **61)** Specifically, the amendment read: "No action may be brought under this subsection [Damages in Civil Action] for the negligent design or manufacture of computer hardware, computer software, or firmware." **62)** To cite just a few: Keysan/Hayes (n. 59) 786; Bruce Schneier, RSA 2012: Are Software Liability Laws Needed?, 1 March 2012, https://www.schneier.com/news/archives/2012/03/rsa_2012_are_softwar.html (arguing that software liability laws are needed to hold software companies accountable for making faulty products); ÖVP Bundesparteileitung, Cyber-Attacken: Rübig fordert Haftung der Softwarefirmen, 16 May 2017, https://www.ots.at/presseaussendung/OTS_20170516_OTS0135/cyber-attacken-ruebig-fordert-haftung-der-softwarefirmen ("a member of the European Parliament requires that software firms be held liable when computer systems malfunction and data is lost due to security loopholes in their software", free translation). **63)** See also the article published in the Economist, Incentives need to change for firms to take cyber-security more seriously, 20 December 2016, http://www.economist.com/news/leaders/21712138-software-developers-and-computer-makers-do-not-necessarily-suffer-when-their-products-go. **64)** Vihul (n. 56), 12. **65)** Michael D. Scott, Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?, 67 Md. L. Rev. 425, 2008, 482, http://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=3320&context=mlr. **66)** Moore (n. 49), 10. **67)** Jennifer A. Chandler, Liability for Botnet Attacks, Canadian Journal of Law and Technology, 2006, 20. **68)** Chandler, Liability for Botnet Attacks (n. 67), 20. **69)** Chandler, Liability for Botnet Attacks (n. 67), 20. **70)** Chandler, Liability for Botnet Attacks (n. 67), 20. **71)** Hewlett Packard, Internet of Things Rese Study; Internet Society, The Internet of Things: an Overview, 23. **72)** Hewlett Packard, Internet of Things Rese Study; Internet Society, The Internet of Things: an Overview, 23. **73)** Moore (n. 49), 10; Vihul (n. 56), 13. **74)** Chandler, Combatting Distributed Denial of Service Attacks (n. 55), 234. **75)** Eric A. Fischer, Cong. Research Serv., Creating a National Framework for Cybersecurity: An Analysis of Issues and Options, 2005, 5–6, http://link.law.upenn.edu/portal/Creating-a-national-framework-for-cybersecurity-/3JfxzsEmjyo/. **76)** Arved Graf von Stackelberg, Haftung und Fahrlässigkeit: Wer verantwortet Cyber-Attacken?, January 2016, http://www.search security.de/meinung/Haftung-und-Fahrlaessigkeit- Wer-verantwortet-Cyber-attacken. **77)** Cem Kaner, Software Liability, 1997, 2, https://pdfs.semantic scholar.org/f03a/cabec45590c8a49737fabfa35727e 5c8cfoe.pdf. **78)** Bruce Schneier, Computer Security and Liability, 3 November 2004, https://www.schneier.com/blog/archives/2004/11/computer_securi.html. **79)** Pinkney (n. 58), 73. **80)** EU Commission Communication "Building A European Data Economy" (n. 50), 4.2. **81)** Thomson Reuters, Calls grow to make IT equipment makers liable for cyber attacks, 30 November 2016, http://www.business insurance.com/article/00010101/NEWS06/ 912310704/ Calls-grow-to-make-IT-equipment-makers-liable-for-cyber-attacks. **82)** Public Consultation on the rules on liability of the producer for damage caused by a defective product, https://ec.europa.eu/docsroom/documents/23541/attachments/2/translations/en/renditions/native. **83)** Moore (n. 49), 10. **84)** Jane Chong, Bad Code: Should Software Makers Pay? (Part 1), 3 October 2013, https://newrepublic.com/article/114973/bad-code-should-software-makers-pay-part-1.