TOWARDS FUNCTIONING PERSONAL DATA BREACH NOTIFICATION IN THE AGE OF INTERNET OF THINGS

Frantisek Kasl

Postgraduate student, Masaryk University, Faculty of Law, Institute of Law and Technology
Veveri 158/70, 611 80 Brno, CZ
frantisek.kasl@mail.muni.cz

Keywords: ***personal data; personal data breach; internet of things; data breach notification***

Abstract: *The mechanism of mandatory personal data breach notification that was introduced beyond the narrow electronic communication sector to all data controllers by the General Data Protection Regulation is facing a new challenge in the form of an omnipresent mesh of interconnected devices processing a wide range of personal data, while at the same time presenting an increasing challenge from the cyber security perspective. The contribution identifies the core features of the internet of things phenomena that complicate or conflict with the concept of personal data breach notification. It further provides a discussion of the available legislative countermeasures.*

1. Introduction

The personal data protection reform brought a greater accent on the accountability of the controller, encouraging greater transparency and security of personal data processing. Partial emanation of this emphasis is the introduction of new general personal data breach notification and communication obligations through the provisions of Art. 33 and 34 GDPR.[1] It can be perceived as one of the reactions to the growing necessity of personal data processing in all segments of the modern society. This is exemplified in particular through the advancement of new technologies collectively often referred to as internet of things. The omnipresence, interconnectivity and adaptability of these personal data processing ICT devices brings about a changing paradigm. The issue explored in this brief contribution is what limitations this change brings for the current approach to personal data breach notification and how to achieve functional setting of the norm in such environment.

2. Personal data breach

At the core of the personal data protection framework is the establishment of adequate measures and procedures by the subject authorized to personal data processing that prevent the occurrence of a detrimental event of the personal data breach. In accordance with Art. 4 no. 12 GDPR, such an event features a «*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.*» It is therefore an undesired, unlawful and often also unintended (from the perspective of the controller, processor and data subject) processing of the personal data. Due to the prevalence of ICT operations in society, the most common (and frequently most damaging) form of personal data breach is a cybernetic incident. As with most «cyber» terms, there is as of yet no unified definition, however, for the purpose of this contribution, the following NIST definition should

[1] 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).

provide adequate qualification: «*Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein.*»[2]

Security of ICT systems is a challenging endeavour that requires continuous reacting to dynamic development of existing and new threats. As such, the possibility of personal data breach in the form of a cybernetic incident cannot be fully eliminated, but merely mitigated to an acceptable and appropriate level. This reality is largely reflected in the obligations of the controller and processor under Art. 32 GDPR.[3] In fact, the increasing volume and severity of disclosed data breaches has established them as a common aspect to be calculated in cost of doing business.[4] This signifies that, in particular small scale, personal data breaches became due to their frequency a rather standard feature of doing business in the modern digitalized society. Despite being slightly exaggerated, a statement by *de Maupeou* nevertheless reflects on current global state of cyber security: «*[t]here are only two types of companies: those who know that they have been attacked and those who don't until it is too late.*»[5] There is a number of security reports indicating a strong trend of continuous increase of variability, frequency and impact of personal data breaches in the form of cybernetic incidents in general and through new technologies in particular.[6] Pursuant to security pattern qualification used by Verizon since 2014, the origins of such breaches can be traced prevalently to infected web applications, crimeware, hacked points of sale, misuse of privilege or authorization, state-sponsored cyber-espionage, payment card skimmers, or denial of service attacks.[7]

3. Regulatory framework for personal data breach notification

The incidents described above can often be strongly distressing from the perspective of the affected individuals, i.e. the data subjects.[8] The European personal data protection regulation provides a strong and complex framework of rights and obligations aimed at establishing a broad adoption of appropriate technical and organisational measures ensuring effective mitigation of the risk of personal data breaches. Nevertheless, the data protection authorities face a challenge in form of functional supervision and enforcement of these obligations on a broad scale.

Personal data breach notification represents a secondary obligation adopted with the aim of increasing transparency towards the data protection authorities as well as the data subjects in order to help mitigate the ensuing damage and the impact of an occurring personal data breach.

The origins of this notification obligation of the controller in case of a non-marginal personal data breach are in the statute adopted in California in 2002.[9] The legal obligation of personal data breach notification is currently present in statutes of all US states,[10] however, the particularities of the framework and resulting

---

2 Cf. Scanlon/Le-Khac (eds.) Proceedings of the 16th European Conference on Cyber Warfare and Security. Academic Conferences and Publishing International. 2017, p. 584.

3 As elaborated on in Recital 83 GDPR.

4 Murray. How to Slay the Hydra: Adopting Charles Ann Wright's the Law of Remedies as a Social Institution as a Framework for Preventing Data Breaches. University of Detroit Mercyla Review 2017, p. 127 (p. 128).

5 Cf. Thales. With Cyberattacks, there are only two types of companies: those who know they have been attacked and those who don't. https://www.thalesgroup.com/en/worldwide/defence/magazine/cyberattacks-there-are-only-two-types-companies-those-who-know-they-have (accessed 7 January 2019).

6 Cf. Gemalto. The Data Breach Index. https://breachlevelindex.com/ (accessed 7 January 2019).

7 Cf. VERIZON. 2018 Data Breach Investigations Report. Executive Summary. https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf (accessed on 7 January 2019) p. 7.

8 Lai/Li/Hsieh. Fighting identity theft: The coping perspective. Decision Support Systems 2012, p. 353.

9 California Security Breach Information Act, Senate Bill No. 1386. Filed with Secretary of State on September 26, 2002. Approved by Governor on September 25, 2002.

10 Boasiako/O'Connor Keefe. The Consequences of Data Breach Disclosure Laws and Disclosed Breaches on Corporate Cash Holdings and Performance. SSRN Electronic Journal 2018, p. 2.

practice is fragmented due to repeated failures to enact a federal law unifying the definition, conditions and form of the notification obligation.[11]

In the EU, on the other hand, this legal instrument was nearly absent until recently, with an exception of the notification obligation for providers of publicly available electronic communications service incorporated in the national laws through the amended Directive on privacy and electronic communications.[12] A major change came on 25th May 2018, when the provisions of the GDPR became applicable. It established through Art. 33 and 34 a unified notification and communication obligation applicable to all controllers.

4. Internet of things

The technological developments surrounding us are advancing on a seemingly increasing pace, bringing into the market and also into common occurrence in our homes, offices and cities continuous stream of new ICT devices. This further contributes to the omnipresent connectivity, constant sensory collection and increasing personal data processing and storage by various interconnected and increasingly adaptable and synchronised items. This trend brings manifestations and consequences well beyond the technology level, contributing to a multi-layered phenomenon broadly discussed and described in academic as well as popular sources. The terminology for this phenomenon is not yet entrenched in a single term or definition. Various authors refer to for example «cyber-physical systems»[13], «ubiquitous computing»[14], «ambient intelligence»[15] or «eObjects».[16] Most popular, however, seems the rather catchy label «internet of things». The broad usage of this term often disguises the variety and divergence in actual content and meaning that it is meant to represent. As can be seen from the comprehensive study of the available definitions elaborated by *Minerva, Biru* and *Rotondi*, the term is often used with a bias towards particular aspects that the author intends to emphasize.[17] They therefore provided a neutral definition reflecting the core and most common features related to the use of the term. As such, the definition differs depending on the scale and complexity of the environment that is being described. From a perspective of small environment with low complexity; «*[a]n IoT is a network that connects uniquely identifiable «Things» to the Internet. The «Things» have sensing/actuation and potential programmability capabilities. Through the exploitation of unique identification and sensing, information about the «Thing» can be collected and the state of the «Things» can be changed from anywhere, anytime, by anything.*»[18] The focus of this definition is to identify particular items and devices as part of the broader network.

For the purpose of this contribution the large environment, complex network scenario definition is more appropriate. In such context the «*Internet of Things envisions a self-configuring, adaptive, complex network that interconnects «things» to the Internet through the use of standard communication protocols. The interconnected things have physical or virtual representation in the digital world, sensing/actuation capability, a programmability feature and are uniquely identifiable. The representation contains information including the thing's identity, status, location or any other business, social or privately relevant information. The things of-*

---

11 Murray. How to Slay the Hydra: Adopting Charles Ann Wright's the Law of Remedies as a Social Institution as a Framework for Preventing Data Breaches. University of Detroit Mercyla Review 2017, p. 127 (pp. 140-141).

12 Directive 2009/136/EC that amended the Directive 2002/58/EC (Directive on privacy and electronic communications) and related Commission Regulation (EU) No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC.

13 Baheti/Gill. Cyber-physical Systems. In: Samad/Annaswamy (Eds.) The Impact of Control Technology. IEEE Control Systems Society, New York 2011, pp. 161-166.

14 Weiser. The computer in the 21st century. Scientific American 1991.

15 Costa. Virtuality and Capabilities in a World of Ambient Intelligence. New Challenges to Privacy and Data Protection. Springer International Publishing, Zurich 2016.

16 Manwaring/Clarke. Surfing the Third Wave of Computing: A Framework for Research into eObjects. Computer Law & Security Review 2015, pp. 586-603.

17 Minerva/Biru/Rotondi. Towards a definition of the Internet of Things (IoT). IEEE 2015. p. 70.

18 Minerva/Biru/Rotondi. Towards a definition of the Internet of Things (IoT). IEEE 2015. p. 73.

fer services, with or without human intervention, through the exploitation of unique identification, data capture and communication, and actuation capability. The service is exploited through the use of intelligent interfaces and is made available anywhere, anytime, and for anything taking security into consideration.»[19] The term in this understanding spans approaches and solutions in multiple varied sectors from healthcare, energy distribution, or infrastructure to retail items for security, convenience or entertainment.[20] As such, the internet of things can be seen as a structural shift in the processes and operations that includes and incorporates the broad scope of more particular new technologies like industry 4.0, smart cars, artificial intelligence, robotics, cloud data storage, blockchains or quantum computing. The defining feature of the concept is not the particular technological form, but the broader impact on data collection, processing, communication and usage. In this way, it is intrinsically interconnected with the framework of personal data protection in these contexts.

5. Ensuing challenges to personal data breach notification

The personal data protection reform was designed and adopted with a full awareness of the new emerging challenges brought by technology development in the fields of ubiquitous computing, cloud computing, artificial intelligence etc. It is partly this intention to future-proof the basic personal data protection rules in a technologically neutral form that stands behind the often criticized vague and abstract language of many GDPR provisions. These foundations provide stable basis for the personal data protection framework, however, specific technological challenges and trends in the modern society may call for further specification and adaptation of the legal framework in order to achieve the goal and purpose incorporated in the general provisions of GDPR.

The above shortly described phenomenon of the internet of things may be an example of such a situation. The transformation of the processes and increased penetration by ICT mesh networks may on one hand present new practical obstacles to exercise of the obligations prescribed by GDPR, but also on the other hand open new possibilities for utilisation of the information collected under the notification procedure.

5.1. Change in frequency and volume of personal data breaches

The expected mass adoption of the internet of things devices in business operations as well as private usage is often viewed with considerable concerns regarding a possible significant increase in cybernetic incidents.[21] The intertwined nature of this new environment is perceived as «threat enhancer»,[22] given that the added complexity is likely to contribute to larger diversity of attack possibilities, while the intrinsic features of many of the devices are likely to make future achievement of sustainable level of cybersecurity in any scenario ever more challenging.[23]

---

[19] Minerva/Biru/Rotondi. Towards a definition of the Internet of Things (IoT). IEEE 2015. p. 74.

[20] Beecham Research Ltd. M2M Sector Map. http://www.beechamresearch.com/download.aspx?id=18 (accessed 7 January 2019), 2011.

[21] Cf. Symantec. Internet Security Threat Report 2017 Volume 22. https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf (accessed 7 January 2019), 2017, p. 64; Arbor Networks. 13th Annual Worldwide Infrastructure Security Report. https://pages.arbornetworks.com/rs/082-KNA-087/images/13th_Worldwide_Infrastructure_Security_Report.pdf (accessed 7 January 2019), 2018, p. 76; Marinos/Belmonte/Rekleitis. ENISA Threat Landscape 2015. https://www.enisa.europa.eu/publications/etl2015 (accessed 7 January 2019), 2016, p. 74.

[22] European Police Office. The Internet Organised Crime Threat Assessment (IOCTA) 2016. European Police Office, The Hague 2016. p. 52.

[23] Schneier. Click here to kill everybody. W.W. Norton & Company, New York 2018. pp. 27-28.

5.2. Change in intensity and form of impact

The internet of things brings in broad sense qualitative transformation of the possible impact of cybernetic incident through the cyber-physical nature of the connected devices.[24] This is most serious with regard to threats to life and health in complex systems like smart cars,[25] but it may be relevant also in context of personal data processing, e.g. through unauthorized activation or manipulation of input collection by devices with cameras or other sensors. A personal data breach is in such scenario literally constituted by the hacked device «spying» on the data subject.

Even disregarding the cyber-physical aspects of the internet of things, the omnipresent interaction with adaptive ICT devices will necessarily lead to more complex and detailed personal data collections and profile databases.[26] Internet of things is the gateway to increased personalisation, optimisation and utilization of new products and services. The accompanying enrichment of infosphere and digitalisation of social interactions is, however, simultaneously likely to change our perception of privacy, secrecy or intimacy. The more of one´s life becomes dependent on virtual identities and digitally provided services, the more damaging and alarming are the future personal data breaches likely to become.

5.3. Change in detection possibilities

As of now, it is unclear if the internet of things represents an environment with better or worse technological possibilities for personal data breach detection. On one hand there are many documented vulnerabilities and security deficiencies in currently available internet of things devices.[27] Even though the full threat potential was yet not utilized, multiple large-scale incidents indicate the growing exposure of fundamental functional networks of our society to external threats,[28] which is also recognized by institutions[29] and organisations[30] responsible for their mitigation.

On the other hand, interconnectivity opens room for better local as well as international cooperation and detection automation, as exemplified by the new capacities of artificial intelligence. This promises more effective responsiveness of the cybersecurity processes.[31]

The technological shift thereby clearly sets new challenges exposing our society to plethora of adverse scenarios, nevertheless, it also provides possible approaches to combat and manage these new threats. It is therefore

---

[24] Software operated actuators and automated decisions with impact on the physical environment are becoming widespread features of the internet of things devices. As such the issue of cyber-physical impact of the systems is therefore broadening beyond the previously closely observed supervisory control systems to plurality of individual devices.

[25] Cf. Greenberg. Hackers Remotely Kill a Jeep on the Highway—With Me in It. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ (accessed 7 January 2019), 2015.

[26] Maras. Tomorrow's Privacy. Internet of Things: security and privacy implications. International Data Privacy Law 2015, p. 101.

[27] Schneier. Click here to kill everybody. W.W. Norton & Company, New York 2018. pp. 30-31.

[28] Cf. Greenberg. The Untold Story of NotPetya, the Most Devastating Cyberattack in History. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (accessed 7 January 2019), 2018; Krebs. New Mirai Worm Knocks 900K Germans Offline. https://krebsonsecurity.com/2016/11/new-mirai-worm-knocks-900k-germans-offline/ (accessed 7 January 2019), 2016; Schneier. New Destructive Malware Bricks IoT Devices. https://www.schneier.com/blog/archives/2017/04/new_destructive.html (accessed 7 January 2019), 2017.

[29] European Police Office. The Internet Organised Crime Threat Assessment (IOCTA) 2016. European Police Office, The Hague 2016. p. 54.

[30] Nist. Considerations for Managing IoT Cybersecurity and Privacy Risks Workshop Summary. https://www.nist.gov/sites/default/files/documents/2018/08/10/considerations_for_managing_iot_cybersecurity_and_privacy_risks_workshop_summary.pdf (accessed 7 January 2019), 2018, p. 3; ENISA. Baseline Security Recommendations for IoT. https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot (accessed 7 January 2019), 2017, pp. 31-35.

[31] Fang/Huang/Li/Li. Position Paper on Recent Cybersecurity Trends: Legal Issues, AI and IoT. In: Au/Yiu/Li/Luo/Wang/Castiglione/Kluczniaket (Eds.) Network and System Security. Springer International Publishing, Hong Kong 2018.

a matter of setting adequate regulatory framework, in order to mitigate the negative impact of the new technologies and promote effective countermeasures.

5.4. Change in the structure of responsible subjects

An important functional aspect of a regulatory framework like the GDPR is a reliable mechanism for the identification of the subject responsible for compliance with the given obligation. Internet of things, as a complex mesh of devices and services with multiple layers[32] often operated and controlled by different subjects or multiple subjects in situation-specific combinations,[33] challenges the clear application of such rules under various provisions of the GDPR. The uncertainty about role allocation with regard to given personal data processing among the multiple partially involved subjects is likely to have detrimental effect on personal data breach reporting. Even now, the compliance with the notification obligation is already facing considerable practical obstacles due to the default incentive structure.[34] An additional ambiguity regarding the accountability of a particular subject for this obligation is therefore strongly challenging the capacity of the norm to achieve its purpose.

6. Discussion

As presented in the previous sections of this contribution, the phenomenon of internet of things is likely to bring transformation of the data processing structures and operations that bring up the question of possible limits of the current personal data breach notification obligation as provided under the GDPR. The core issue at hand is whether the currently available legislative expression of the norm shall remain sufficient for achievement of its normative purpose in the complex environment of the internet of things. The purpose pursued by this norm is largely connected with its form as secondary obligation to the duty to provide adequate protection of personal data processing. As the norm is triggered by an event with adverse impact on the personal data, the principal purpose lies in the minimisation of the resulting damage through alleviation of the informational asymmetry of the data protection authority and eventually also the affected data subject.

It must be therefore considered what obstacles ensue from the internet of things phenomenon for the capacity of the norm to contribute to such damage mitigation. The most significant of these can be derived from the changes likely connected with this technological shift as described in the previous section.

The higher penetration of society with interconnected personal data processing ICT devices vulnerable to cybernetic incidents increases the overall urgency of adequate protection measures and benefits from functioning data breach notification structure. The higher diversity and frequency of such incidents then increases the burden of the responsible subjects to implement effective monitoring and reporting tools and procedures, which may disproportionately encumber certain types of controllers, in particular, if they additionally count among the small and medium enterprises.

An increased impact of personal data breaches connected with the cyber-physical nature of the internet of things and higher reliance and exposure of individuals to the digital personal data processing fortifies the need for transparency, but also for rapid identification and communication of the incident to the authority and the

---

32 The primary layer includes the sensors, data collection and controlling modules and other perception aspects of the devices. The connectivity then presents a distinct layer ensuring the data transmission over various communication protocols and network overlays. The specific data processing and services provides by or through the devices then from the application layer. Cf. Yang/Li/Geng/Zhang. A Multi-layer Security Model for Internet of Things. In: Wang/Zhang (Eds.) Internet of Things. Springer Berlin Heidelberg 2012, p. 389.

33 The plurality of subjects participating on the data collection, transmission and processing is likely to lead to frequent establishment of jointed controllers' relationships. Additionally, the automated machine to machine communication protocols and increasing role of artificial intelligence in various processes suggest future need for more dynamic role allocation and responsibility distribution.

34 The relevant adverse factors in consideration of the data breach notification compliance include the impact of potential future litigation, regulatory penalties or reputation damage. Cf. Boasiako/O'Connor Keefe. The Consequences of Data Breach Disclosure Laws and Disclosed Breaches on Corporate Cash Holdings and Performance. SSRN Electronic Journal 2018. p. 3.

data subject. The crucial nature of this factor is further highlighted by current level of average delay between personal data breach and its detection and disclosure by the controller.[35]

The incentives for rigorous and timely compliance with the notification obligation need to distinctly exceed the eventual counter-incentives for omission or obscuring of the detrimental event. In this context is relevant not only the normative content of the provision, but also the functioning of the existing mechanisms for its application and enforcement.[36]

A large obstacle can be further perceived in the increasingly complex network of subjects involved in some aspect of the personal data processing under the internet of things. With the increased frequency of situations, where the distribution of accountability and responsibility for particular obligations like the personal data breach notification can be deemed ambiguous under the current legal framework, the counter-incentives for omission or obscuring on part of participating responsible subjects may be inappropriately strengthened.

Consequently, the major limitations for the appropriate compliance with the personal data breach notification obligation pursuant to the GDPR under the internet of things identified in this contribution are threefold: (i) frequent ambiguity with regard to accountability; (ii) relatively weak incentives for compliance joined with limited enforcement possibilities in case of non-compliance; and (iii) an increase of disproportionate burden for certain categories of controllers.

The possible regulatory solutions for these challenges should combine multiple instruments and approaches. Some of these are mentioned in the following paragraph; however, each is rather a keyword encompassing a complex structure with multiple aspects that require careful consideration and determination.

A more refined clarification of appropriate measures for personal data protection through references to security standards or introduction of obligatory cybersecurity conformity certification for internet of things devices may have strong indirect benefits for personal data breach notification through clarification of requirements and enforced adoption of adequate monitoring tools. A regulatory framework for joined accountability and accountability distribution in the case of dynamic processes would ease the obligation assignment to the multiple participating subjects. Clarification and readjustment of responsibility for processes operated by artificial intelligence and automated machine-to-machine communication could bring additional benefits in more complex scenarios. Modification of the personal data breach notification obligation into sectoral information sharing structures with data protection authority supervision may reinforce the incentives for compliance through more evident benefits for the responsible subjects, which is also likely to benefit the data subjects. Furthermore, if taken from a broader perspective, a better legislative coordination with the notification obligations towards authorities responsible for cybersecurity and cybernetic incident reporting could alleviate some of the disproportionate burden on certain categories of controllers.

7. Conclusion

The internet of things represents a complex phenomenon with broad impact on the modern informational society and its legal framework. Due to the crucial role of personal data processing in the future processes and operations, the consideration of suitability of the current personal data protection framework is timely. The personal data breach notification obligation under the GDPR is an example of a norm that may benefit from adjustment with regards to challenges posed by the internet of things. These result in three major limitations for the capacity of the norm to contribute to personal data breach damage mitigation: (i) frequent ambiguity with regard to accountability; (ii) relatively weak incentives for compliance joined with limited enforcement possibilities in case of non-compliance; and (iii) an increase of disproportionate burden for certain categories

[35] A mean time to identify a data breach was in 2018 based on data from Ponemon at 197 days. Cf. Ponemon Institute. 2018 Cost of a Data Breach Study: Global Overview. IBM 2018. p. 33.

[36] Cf. Garcia. The Economics of Data Breach: Asymmetric Information and Policy Interventions https://etd.ohiolink.edu/ap/10?0::NO:10:P10_ACCESSION_NUM:osu1365784884 (accessed 7 January 2019), 2013, p. 180.

of controllers. A combination of regulatory measures may be required to overcome these obstacles, some of which were mentioned in this contribution.

8. References

Boasiako, Kwabena Antwi/O'Connor Keefe, Michael. The Consequences of Data Breach Disclosure Laws and Disclosed Breaches on Corporate Cash Holdings and Performance. SSRN Electronic Journal 2018.

Baheti, Radhakisan/Gill, Helen. Cyber-physical Systems. In: Samad/Annaswamy (Eds.) The Impact of Control Technology. IEEE Control Systems Society, New York 2011.

Costa, Luiz. Virtuality and Capabilities in a World of Ambient Intelligence. New Challenges to Privacy and Data Protection. Springer International Publishing, Zurich 2016.

Enisa. Baseline Security Recommendations for IoT. https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot (ac-cessed 7 January 2019), 2017.

European Police Office. The Internet Organised Crime Threat Assessment (IOCTA) 2016. European Police Office, The Hague 2016.

Fang, Junbin/Huang, Yun Ju/Li, Frankie/Li, Jing. Position Paper on Recent Cybersecurity Trends: Legal Issues, AI and IoT. In: Au/Yiu/Li/Luo/Wang/Castiglione/Kluczniaket (Eds.) Network and System Security. Springer International Publishing, Hong Kong 2018.

Garcia, Michael E. The Economics of Data Breach: Asymmetric Information and Policy Interventions https://etd.ohiolink.edu/ap/10?0::NO:10:P10_ACCESSION_NUM:osu1365784884 (accessed 7 January 2019), 2013.

Lai, Fujun/LI, Dahui/Hsieh, Chang-Tseh. Fighting identity theft: The coping perspective. Decision Support Systems 2012.

Manwaring, Kayleen/Clarke, Roger. Surfing the Third Wave of Computing: A Framework for Research into eObjects. Computer Law & Security Review 2015.

Maras, Marie-Helen. Tomorrow's Privacy. Internet of Things: security and privacy implications. International Data Privacy Law 2015.

Marinos, Louis/Belmonte, Adrian/Rekleitis, Evangelos. ENISA Threat Landscape 2015. https://www.enisa.europa.eu/publications/etl2015 (accessed 7 January 2019), 2016.

Minerva, Roberto/Biru, Abyi/Rotondi, Domenico. Towards a definition of the Internet of Things (IoT). IEEE 2015.

Murray, Tanya. How to Slay the Hydra: Adopting Charles Ann Wright's the Law of Remedies as a Social Institution as a Framework for Preventing Data Breaches. University of Detroit Mercyla Review 2017.

Scanlon/Le-Khac (eds.) Proceedings of the 16th European Conference on Cyber Warfare and Security. Academic Conferences and Publishing International. 2017. ISBN: 978-1-911218-44-9.

Schneier, Bruce. Click here to kill everybody. W.W. Norton & Company, New York 2018.

Weiser, Mark. The computer in the 21st century. Scientific American 1991.

Yang, Xue/Li, Zhihua/Geng, Zhenmin/Zhang, Haitao. A Multi-layer Security Model for Internet of Things. In: Wang/Zhang (Eds.) Internet of Things. Springer Berlin Heidelberg 2012.