Internet of Things - Assessment of Incentives of Businesses to Fulfil the Personal Data Breach Notification Obligation under the proposed General Data Protection Regulation

Frantisek Kasl
Masaryk University, Faculty of Law, Institute of Law and Technology, Czech Republic

ABSTRACT
The contribution is aimed at discussing the issues related to data protection in context of the Internet of Things. In this respect there is firstly provided an introduction into the concept of the Internet of Things. It is followed by an overview of current tendencies in cybersecurity and personal data breach reporting. Subsequently the newly adopted European General Data Protection Regulation is discussed with focus on the general mandatory personal data breach notification obligation. The specifics of the Internet of Things in this context are also considered. The final section then attempts to encapsulate available economic models relevant for this issue.

KEYWORDS
Internet of Things; data protection; personal data breach; General Data Protection Regulation

Introduction
This paper is based on the project of a dissertation with similar scope. It does thereby serve as an introduction to the topic, as it shall be further developed in the doctoral paper. The attention is concentrated on the new obligations related to personal data breach under the General Data Protection Regulation. These shall be analysed from legal as well as economic perspective with emphasis on the applicability on the emerging environment of the Internet of Things.

Internet of Things
The Internet of Things connects through the global network even such items, which we would never imagine could go online. The analysts predict that the Internet of Things will represent one of the most significant changes in ICT of the next decade.

1 Author is a doctorate student at Masaryk University, Faculty of Law, Institute of Law and Technology, Czech Republic with a dissertation project on the topic Legal and economic aspects of personal data breach in the context of Internet of Things. He has a educational background in law and in economics. Contact: frantisek.kasl@gmail.com

The concept, as well as the term, has been around for some time now, yet recent developments are putting this trend more and more often into the spotlight. The increased connectivity of items leads to a steady increase in the global machine-to-machine data traffic. There are a great number of new devices introduced to the market, sold and connected to the networks every day and the number is expected to only grow faster. To gain the proper perspective of technological changes well underway at this moment, we need to realize that development in this field is strongly influenced by the so called "Moore’s law" of exponential improvement.

The scope of areas which are being transformed by this new technological trend is ever-increasing. From commercial applications in industrial automation, logistics, retail or resource management through public domains like healthcare, research, energy distribution, public safety or infrastructure to numerous private consumer uses in safety, convenience and entertainment areas, there are countless examples of devices to be found, which are to be regarded as part of the Internet of Things.

Increased attention in the public sector is devoted to the prospects of urban infrastructure with significant involvement of various sensors to increase efficiency of various integral systems (traffic density, pollution, water and waste management, street lightning, energy distribution etc.); area commonly labelled as "smart cities". The most currently frequented topic related to the Internet of Things (thanks to a surprisingly successful release of smartphone game based on Japanese cartoon series) is the prospect of merging the real and virtual world, so called “augmented reality”, an omnipresent coverage by information networks, which becomes unavoidable (and unescapable) part of the common perception of the world around us.

It is difficult to avoid the feeling that there are hardly any areas of our lives or society, which will not be affected by the integration of “smart” devices. We can therefore assume that there will potentially be “smart” alternatives for any commercially feasible item, as long as there will be markets for them or there will be other benefits to be derived from

---

3 Probably the first well documented „smart thing“ connected to the Internet was coffee pot at the University of Cambridge on 22.11.1993. For more details see: KESBY, R. How the world’s first webcam made a coffee pot famous. BBC News [online]. 22.11.2012 [25.7.2016]. Available at: http://www.bbc.com/news/technology-20479101


their production (internal enterprise savings, new marketing possibilities, more customer data, increased efficiency etc.).

As can be derived from the description in the previous paragraphs, the Internet of Things represents a rapidly developing technological phenomenon, which is constantly undergoing changes and new breakthroughs. Nevertheless, suitable general definition for the purpose of this paper can be as follows: “The Internet of Things is a concept whereby any item can connect to the Internet to retrieve information to enhance its intrinsic value. The scope of the Internet of Things (IoT) is therefore very broad. It includes communicating devices and M2M but it aims to go beyond M2M, by enabling any object to connect and leverage the Internet (the Internet of Objects), even if it does not contain the electronics required to connect directly to the Internet (use of an intermediate device.).” Communicating devices refers to devices, which have connectivity as their primary feature (e.g. smartphones, tablets), whereas M2M (machine to machine) are objects with autonomous functions, which are enhanced by communication module for the purpose of automated communication with the server or other machines (e.g. smart fridge, gadgets, TVs, cars, thermostats, medical devices). The Internet of Objects is a label for items that do not collect data, but contain ID technology (most common are RFID and 2D barcodes), which allows them to openly communicate imbedded information about themselves (e.g. packaging, reusable transport items, access cards). This paper is primarily dealing with issues related to devices capable of active communication, which are represented by the two former groups described in this paragraph.

This active communication between interconnected items means that they are sharing immense amounts of data (including personal data related to behaviour and description of its users). Such online data traffic may lead to very fundamental breaches of private sphere and continual surveillance in a form of personal data collection. This leads to the related phenomenon labelled “big data”. This term is used for large volumes of structured, semi-structured or unstructured as well as personalized, pseudonymized or anonymized data, which are amassed in a database and provide the opportunity for data mining. Data mining means filtering and combining data in order to identify patterns and detect relationships between them in order to create systematically indexed databases. These can in turn be used for countless purposes, including profiling of users, consumer behavioral analysis, and analytical decision-making.

---


14 For more detailed description see ROUSE, Margaret. An admin’s guide to AWS data management. Definition big data [online]. July 2014 [25.7.2016]. Available at: http://searchcloudcomputing.techtarget.com/definition/big-data-Big-Data

15 For more see e.g. FREITAS, Alex A. Data mining and knowledge discovery with evolutionary algorithms. Springer Science & Business Media, 2013, ISBN: 9783662049235.
supply chain efficiency management, online identity theft, surveillance or espionage.\textsuperscript{16} Big data is in many ways specific with regard to risks and dangers of data breaches as it usually represents massive databases of personal or in other way valuable data. This is also a reason, why it historically stands behind largest data breach incidents and represents the majority of cases of attempted data breach. The recent reports, however, show that this trend is shifting, with more personal devices and individual users being targeted by data breach attempts than servers storing the massive databases, which practically represent the big data.\textsuperscript{17} This development may reflect shifts in technological trends, combined with increased security measures in enterprises maintaining the databases of big data (e.g. cloud providers, social media providers, search engines, banks). This may foreshadow an increasing role of increasing penetration, and thereby relevance from the perspective of data security, of Internet of Things devices. There are only limited data breach examples featuring such devices in previous years, but there are also indications that this may be already changing. The Internet of Things devices usually are not or cannot be designed with high data security build in them, which is why their increasing omnipresence may make them into attractive targets for data breach attempts.\textsuperscript{18}

\section*{Data breach}

As outlined in the previous section, the Internet of Things represents a novel field of technological possibilities, which can and should be assessed from all possible angles. The topic of this contribution is the potential of the security risk connected with the rise of this new area of online connectivity. We already live in a digitally interconnected world, which is in constant struggle for data security. This combat is led on every access point to a network and the rise of the Internet of Things creates numerous new fronts that can be assaulted, contaminated, penetrated or taken advantage of in order to gain access to the data within a network.

ISO/IEC 27040 contains following definition of data breach: “Compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored or otherwise processed.”\textsuperscript{19} Ponemon Institute repeatedly identified three root causes of data breach: malicious or criminal attack; system glitch; or human error, whereas hackers and criminal insiders were identified to have caused the significant majority of analysed data breaches.\textsuperscript{20}

There is a notable shortage of data regarding data breaches overall as well as in specific jurisdictions. The reasons may lie with generally limited notification obligations or compliance with such, as any enterprise notifying a data breach is usually facing a significant risk of damage to its reputation, if publicly identified as a subject of personal data breach. There are several well established annual reports provided mainly by research institutes support-
ed by key players in the cybersecurity industry, but it needs to be taken into consideration that these reports are mostly based on limited data sources from each jurisdiction concerned. They do, nevertheless, provide valuable insight into the current situation on the cybersecurity battlefront. These reports aspire to provide general overview of the global situation, as well as comparisons between various regions and jurisdictions, but given the limited data available, only general trends and conclusions shall be considered for the purpose of this contribution.

Verizon identified in its 2016 report that majority of personal data breaches come from external actors (meaning hackers), who have primarily financial motives and who increasingly rely on phishing (fraudulent personalized messages aimed at tricking the recipient) or keylogger/spyware malware (malicious software aimed at recording keystrokes or other activities on the device).21

The report by Symantec informs about the largest data breach up to date from December 2015, when 191 milion records were exposed, bringing the total number of data breaches exposing 10 million or more records to 9 in 2015 alone.22 It further stresses the significant increase in phishing attacks and ransomware attempts (encryption malware that requires payment to prevent the data from being deleted), both aimed at personal devices or company devices operated by employees.23

Ponemon Institute annually models a probability estimate of personal data breach per business entity based on its available data. There is a noticeable growth trend, as the estimated likelihood of data breach in an enterprise with a size of at least 10 000 exposed records in the period of the next 24 months increased from around 22 % in 201424 through about 24 % in 201525 to almost 26 % in 2016.26 The previous reports hint towards a conclusion that the likelihood and impact of cybercrime and data breaches is increasing. This estimate is further elaborated on in the report by McAfee, which identifies cybercrime as growth industry that is likely to benefit from the new opportunities created by vulnerabilities in the Internet of Things devices. It highlights that global cybersecurity is about challenging the growth of cybercrime by improved defences and better international cooperation.27 There are various promising technological advances, which might increase the efficiency of the cybersecurity.28 However, technological advances are to similar degree responsible for improved cybercrime attacks. It is there-

---

fore the organizational aspects of cybersecurity, which promise opportunities to improve the overall situation and part of them is the applicable legislative framework.

One of the most prominent legislative tools to combat data breaches is the introduction of data breach notification obligations. These generally aim to increase overall cybersecurity by detecting and analysing the vulnerable entities as well as indirectly influencing entities towards improving their cybersecurity. The main justification for such regulation is seen in the negative externalities of data breaches,\(^29\) which besides generating costs for the directly affected entity further transmit to other entities due to the interdependent nature of information and communication networks.\(^30\)

**Bringing the European data protection into the 21st century**

Protection of personal data is intensively pursued in the European Union since the dawn of commercial internet, leading to early adoption of the Data Protection Directive 95/46/EC (“DPD”),\(^31\) which is the basis for minimal data protection threshold throughout the Single Market. The level of protection throughout the European Union is, however, unequal, as each member state establishes its own national data protection laws. Significant role is played by various branch specific laws and regulations, which provide for special obligations for entities active in those fields (banking, telecommunications, internet providers etc.).

The national regulations of personal data breach vary, whereas only three member states have currently in place an advanced framework for personal data breach reporting by entities processing personal data in general (Germany\(^32\), Netherlands\(^33\) and Ireland\(^34\)), but even these notifications are mainly limited to larger data breaches targeting sensitive personal data. The majority of member states have only implemented the Directive on privacy and electronic communications,\(^35\) which requires personal data breach notification by *providers of publicly available electronic communications services* (e.g. internet access providers).\(^36\)

---


33 Ibid, page 322.

34 Ibid, page 209.


The provisions of DPD come from an era before the widespread usage of internet and modern technologies, which provide previously unexpected scope of virtual traffic. It is therefore more than welcome that in two years time it shall be replaced by the General Data Protection Regulation (“GDPR”), which was published in the Official Journal of the European Union on 4th May 2016 and shall enter into force on 26th May 2018.37

Parallel to the GDPR come into existence also further national and European projects aimed at increased cybersecurity, most distinctively the Directive on security of network and information systems (“NIS Directive”), published in the Official Journal of the European Union on 19th July 2016 and coming into force in August.38 This directive is aimed at digital service providers (e.g. online search engines, cloud computing providers, or online marketplaces) and operators of essential services (e.g. gas and electricity suppliers, airlines, credit institutions, health care providers, drinking water supply and distribution, or digital infrastructures).39 These shall be among other things obliged to notify to the competent authority without delay security incidents40 having a significant impact on the continuity of the essential services they provide.41 The competent authority has possibility to publicize the incident, if given conditions are met.42 The NIS Directive and the GDPR shall potentially overlap by security incidents, which involve personal data breach.

**Impact of the Internet of Things on the area of data protection**

Given that the security must be effective on every access point and by every entity processing or collecting given set of data, it is of high significance to create a legal framework that can establish and enforce such widespread data security. Such goal is more realistic to be achieved, if the data protection authority (“DPA”) is aware of security failures (in this case personal data breaches) and can thereby detect the most vulnerable part of the network.

The Internet of Things itself does not directly affect the obligations related to data breach, given that they mainly fall under area covered by the currently applicable general concepts and definitions of data protection law. However, several aspects of the Internet of Things bring new and escalating challenges to the current data security and thereby also to its legal framework.

Firstly, the collection and processing of data under the Internet of Things presents probably the most discussed legal aspect of this new trend. One of the main challenges is the security of such data (which can have personal nature or provide opportunities to be combined into data with personal nature), given the limited technological possibilities as well as oth-

---


39 Article 1 paragraph 2 letter d) NIS Directive.

40 “[…] any event having an actual adverse effect on the security of network and information systems.” Article 4 paragraph 7 NIS Directive.

41 Article 14 paragraph 3 and Article 16 paragraph 3 NIS Directive.

42 Article 14 paragraph 6 and Article 16 paragraph 7 NIS Directive.
er practical problems (e.g. limited battery and memory prohibits regular security patches or difficult accessibility of the “smart” chip embedded into “smart city” infrastructure eliminates the possibility of hardware update).

Secondly, newly connected items with limited cybersecurity and update possibilities may create new vulnerable points of access into a number of networks (single vulnerability can be exploited in many similar devices, if these devices cannot be easily and quickly patched), increasing the likelihood of effective malicious attack and subsequent data breach.

Third challenge is in the adaptation of the technological reality to the legal framework. The rising use of interconnected devices, which collect and process increasing variety of personalized data, will subject various new entities (e.g. small business owners, start-ups, non-profit organisations) to the strict personal data protection regulations. The increasing ubiquity of Internet of Things can at the same time present difficulties for precise legal assessment, as the networks of devices with get ever more complex, creating a challenge for accurate notifications of data processing activities (and potentially punishing the dutiful many rather than the dishonest few).

Combining all former aspects, the biggest challenge presented by the Internet of Things is probably the increasingly autonomous nature of machine-to-machine communication, which presents new uneasy questions about responsibility, accountability, supervision, accessibility and other practical aspects of the application or enforcement of the data protection law, also in relation to the data breach notification obligation.

**GDPR and general personal data breach notification obligation**

The GDPR promises a significant update to the level of data protection throughout the European Union as well as unification of the general national level of personal data protection (branch specific laws and regulations will remain unaffected and therefore inhomogeneous). The GDPR newly provides for a unified level of general reporting obligation by controllers in case of personal data breaches, which builds on the frameworks introduced by the three above mentioned member states and in some regards even goes beyond.

GDPR contains a significant broadening of the personal data breach reporting obligations towards the supervisory authority, encompassing virtually all controllers, whereas the notification period is maximum 72 hours after becoming aware of the personal data breach.\(^{44}\) This shall lead to application of reporting obligations also to cases including the items connected to the Internet of Things, which can happen more often than expected, given the limited possibilities for firewall patching or system update on many of these items. To avoid the “swamping” of the supervisory authority by reports of minor data breaches, exception is given to cases, which probably do not represent a risk to the rights and freedoms of individuals.\(^{45}\) It is however unclear, where is the line to be drawn, and this definition should be the subject of further implementing legislation. It is likely, given the ability to personalize and profile users as well as provide sensitive data regarding behaviour, life pattern or individual features in case of the more sophisticated items connected to the Internet of Things, that breach of their security will be classified as such risk.

---

\(^{43}\) Generally an entity, which, alone or jointly with others, determines the purposes and means of the processing of personal data. Article 4 point 7 GDPR.

\(^{44}\) Article 33 paragraph 1 GDPR.

\(^{45}\) Ibid.
GDPR further sets down notification obligation directly towards the data subject, whose data were affected, in cases, when the personal data breach represents a high risk for the rights and freedoms of individuals.\(^{46}\) This, however, is not required in cases, when the data affected were appropriately protected, in particular through encryption or if the controller took subsequent measures, which ensure low likelihood of materialization of the high risks to the affected data subjects.\(^{47}\) If the communication to the data subjects is on the other hand merely disproportionately difficult, the controller is obliged to make the personal data breach public.\(^{48}\)

The scope of applicability of these obligations on the personal data breach featuring Internet of Things device is not easy to define. As mentioned above, connected item may take on many forms and process or collect various types and combinations of data, personal or otherwise. Given the broad definition of personal data in GDPR,\(^ {49}\) it is up to implementing acts and case law to define specific boundaries of sensitive personal data, personal data, pseudonymized data, anonymized data and other groups, which are central to the European data protection law. There is, of course, considerable experience with the equal definition of personal data under the DPD and within national jurisdictions of each member state, but the Internet of Things brings a variety of new forms of data, which must be assessed with regard to the current understanding of personal data, given their deeply personal nature and potential for combination with other data.

The concept of fines with high ceiling under the GDPR may cause uncertainty on the part of the personal data controllers (especially the small and medium businesses). Violation of above described notification obligations, as well as many other obligations under the GDPR, is subject to administrative fine of up to 10 000 000 EUR, or in case of an undertaking, of up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.\(^ {50}\) Such possibilities for sanctions seem in stark contrast to the ever-changing technological reality of the Internet of Things. The scope of their application by the DPAs will probably have a defining impact on the perception of the GDPR as a whole.

The GDPR shall introduce a shift in personal data breach notification obligations as well as provide means for enforcing the new regulation. Nevertheless, current mandatory data breach notification systems show only limited levels of compliance. It is therefore uncertain, whether the GDPR personal data breach notification obligation will be complied with or rather whether it is in practice enforceable by the DPAs in order to ensure such compliance.

There are voices\(^ {51}\) considering the GDPR inapplicable on the practical environment of current processing, sharing and collection of data, due to reasons ranging from complexity of

\(^{46}\) Article 34 paragraph 1 GDPR.

\(^{47}\) Article 34 paragraph 3 letter a) and b) GDPR.

\(^{48}\) Article 34 paragraph 3 letter c) GDPR.

\(^{49}\) ‘personal data’ means 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. Article 4 point 1 GDPR. The definition is equal to current definition under the DPD, whereas the Court of Justice of the European Union continually stretches the interpretation of this definition.

\(^{50}\) Article 83 paragraph 4 GDPR.

data controllers clusters to overburdening both DPA and data subjects with information. The new framework under GDPR shall no doubt present great challenge for controllers and DPAs alike. The regulation enshrines values and principles, which do represent the manifestation of European values in the digital environment: transparency, data limitation, security and accountability. Yet these values must manifest through enforceable rights and freedoms of the data subjects, which require a law that provides the DPAs with sufficient authority to effectively enforce the obligations on the controllers, but that also provides clear and intelligible instructions for the controllers regarding their required behaviour. There remains a wide area to be covered by sector specific guidelines and recommendations to enhance the legal certainty for the controllers as well as for the data subjects.

With regard to the data breach notification, such interpretation materials require among other things the understanding of risk assessment and decision making of business entities in relation to the notifications of personal data breach.

**Economic approach to personal data breach**

The decision most of the business entities take in regard to notification and disclosure of personal data breach is economic in nature. Personal data breach represents an incident with negative impact, where the decision between disclosure and non-disclosure takes the form of choosing the probably less costly approach. The main risks connected with personal data breach include costs related to the loss of data, risk of damaged reputation, loss of market capitalization, increased insurance premium or risk of lawsuits for damages caused by the personal data breach. Unreported personal data breach may further lead to sanctions from the supervisory authority following a security audit.

There are various previous applications of economic models on the challenges faced by business entities in relation to cybersecurity and optimal security investment in the face of data breaches. These provide a starting point for economic approach to understanding incentives of the enterprises involved in the personal data breach situations.

Highly accepted is the *Gordon-Loeb model*, which is aimed at defining the optimal investment level into cybersecurity. The model is based on the presumptions that firms are challenged with constant level of threat they cannot influence, but their additional investments in information security may decrease the vulnerability of their information sets. However, the investments function is a function of diminishing returns, as the information set cannot be made perfectly secure with any finite investment into security. The model consequently identifies an optimal amount of investment in information security, defined as maximized difference between benefits (i.e. decrease in vulnerability) and costs. The optimal amount is tested on various levels of vulnerability (i.e. expected value of information loss). Contrary to common expectation, the model shows that investments should not be an increasing function of the vulnerability, as the effect of increased investment in securing highly vulnerable information sets is too small to be economically optimal. The

---

52 Article 5 GDPR.
model also, under additional assumptions, sets the maximal amount of the security investment below 37% of the expected loss due to the data breach.55

The conclusions reached in the model shed some light on the basic motivations of an enterprise regarding security investment in face of data breach. The budget constraints lead to search for the most optimal expenses on security with regard to cost-benefit difference, rather than maximal security of the most vulnerable data sets. This, however, does not accurately reflect the market reality, as there are regulations and additional requirements, which are aimed at increasing the security of certain data sets (e.g. sensitive personal data) despite the diminishing returns on investment. The general conclusions of the Gordon-Loeb model do, however, retain validity, as confirmed by Yuliy Baryshnikov,56 who simultaneously pinpointed constraints of the model and of its applicability.

There is a large follow-up research based on the Gordon-Loeb model or dealing with related issues from new perspectives.57 Most of the research papers represent partial building blocks for how to deal with the issue concerned in this contribution, do not, however, focus specifically on the issue.

The limit of the Gordon-Loeb model was in omitting the regulatory obligations of the enterprise with regard to data breach. Central to them is the already mentioned personal data breach notification, which calls for wholly different decision making process within the enterprise. This decision process regarding compliance with the personal data breach notification obligation was modelled by Michael Erik Garcia58 in his dissertation. The model is based on the US regulatory and enterprise framework, which, however, does not preclude from deriving certain general conclusions for the purpose of this contribution.

55 Ibid, page 452.
Michael Erik Garcia attempts to present a more comprehensive model than those previously mentioned, as well as to include the social consequences of the enterprise's choices. Importantly, the model is based mainly on imperfect enforcement, due to which the enterprise may choose not to report the data breach, but does not necessarily have to be caught doing so (i.e. there is potential benefit in not complying with the obligation). The economic justification behind doing so represents one of the crucial aspects analysed by the model.

First conclusion is that the policymaker cannot effectively end all data breaches; it should rather concentrate on market inefficiencies.59 Secondly, considering only enterprise's incentives (as in the Gordon-Loeb model) leads to underinvestment into information security relative to the social optimum, because interdependencies and negative externalities need to be also considered.60 These conclusions justify regulatory interventions in order to incentivize the socially optimal level of investment. The model deeply analyses the role of information asymmetry regarding data breach within the enterprise towards the regulator as well as moral hazard on the side of the enterprise in the face of potential fines for non-reporting.61 Additional aspects like potential reputation costs, externality market failures, disclosure policies are also taken into consideration. The model shows the influence of certain regulatory burdens connected with disclosure policy and non-reporting fines62; nevertheless the conclusion is in favour of such policies, as long as the expected regulatory burden does not surpass the benefits from additional security investment related to the regulatory effect.63

Furthermore, recent paper by Stefan Laube and Rainer Böhme64 focused directly on the effects of mandatory personal data breach reporting on the information security, or more precisely on how to adjust the level of sanctions for non-reporting in order to achieve socially beneficial regulation. It introduces a model for principal-agent problem with moral hazard. The principal represents the regulator and the agent the enterprise obliged to notify data breach. The moral hazard is connected with the potential benefits of non-compliance with the notification obligation. “[The] model consists of three different components: a model for security investment and interdependent security, a formalization of mandatory security breach reporting to an authority, and a formalization of security audits.” 65 Various effectiveness levels of authority security audits are considered and Nash equilibrium is identified. The authors claim that high audit probability has to be avoided, yet audits may incentivize security breach reporting. A balance function for efficiency of audits is proposed.66 They further claim that “the enforcement of mandatory security breach reporting to an authority is effective in case of high interdependence between agents, low disclosure costs associated with security breach reporting, a high effectiveness of an informed authority in dissemination of knowledge to agents, and a low error rate of detective controls.” The main

60 Ibid, pages 67-68.
61 Ibid, pages 70-105.
The conclusion of this research is that sanctions do not provide sufficient incentive for personal data breach notifications by majority of the business entities, unless accompanied with regular security audits by the DPA. However, the regulatory system is prone to misadjustments of the security audits’ probability and level of sanctions, which may lead to over-regulation, further resulting in internalizing of negative externalities of the data breach by the enterprises. The potential of tradeoff between the frequency of security audits and severity of the sanctions is considered, but negative effects on firms which do not report security breaches because of benign nescience are highlighted.\(^\text{67}\) This actually represents the challenge connected with the application of the GDPR data breach notification obligations on the everchanging network environment of the Internet of Things. This challenge shall be addressed further in the doctoral paper.

**Conclusion**

The Internet of Things represents a new data protection frontier, which brings new challenges for the data controllers and DPAs alike. GDPR will introduce new general mandatory personal data breach notification obligation, which is currently regulated only in a few member states. The changes are aimed at increasing data security by data controllers without differentiation, however, clear and understandable guidelines need to be created to help entities understand and follow their new obligations. The incentives of entities to fulfil these reporting obligations are an open question, but experiences from jurisdictions with standing mandatory data breach notification obligations should provide materials for better understanding of business rationale and help identify crucial aspects affecting the compliance with the new notification requirements as well as possible impact on cybersecurity investments.

The research presented in the last section includes very well devised general models for the behavior of an enterprise in regard to security investment and data breach regulation. They provide insight into the internal decision processes and economical reasonings behind their decisions, when faced with the general threat of data breach. The models are, however, intended to greatly simplify the settings to highlight the general rules and principles hidden behind the economically optimal decision making. They usually work with concept of data breach threat and regulatory authority behaviour and efficiency that do not effectively mirror the reality. The question how to provide an effective assessment of the mandatory data breach notification regulation in the context of the expansion of the Internet of Things remains largely untackled by these models. Therefore the aspiration towards more precise understanding of the optimal enterprise behaviour as well as socially optimal regulatory settings in this area shall guide my further research.

**REFERENCES**

- BARYSHNIKOV, Yuliy. IT Security Investment and Gordon-Loeb’s 1/e Rule. [online] Departments of mathematics and ECE, UIUC, Urbana, IL, 2012

\(^{67}\) Ibid, page 19.


