THE US LESSONS FOR THE EU PERSONAL DATA BREACH NOTIFICATION: PART I – WHAT IS PERSONAL DATA BREACH AND INTRODUCTION OF THE US REGULATORY PERSPECTIVE

František Kasl*

Abstract: *The new obligation to notify personal data breaches under Articles 33 and 34 of the General Data Protection Regulation 2016/679 can be seen as a reflection of the US regulatory approach to security breach incidents, which has an established tradition since the enactment of Security Breach Information Act in California in 2002. The contribution presents in two parts the relevant legal frameworks of the US and the EU, in order to provide a discussion on their similarities and differences. The aim is to identify available intellectual stimuli to the respective academic debate regarding interpretation, application and specification of the EU provisions based on inspiration from the US experience. The Part I introduces the reader to the concept of personal data breach and its relevance in nowadays digital society and then offers and introduction of the relevant US regulatory frameworks.*

Keywords: *Personal data breach, security breach, notification obligation, US law, GDPR*

1 INTRODUCTION

The negative side-effect of the increasing dependence of the modern society on digitalized communication and data storage is growing susceptibility to malicious or accidental breach of data security. The past decade provided numerous examples of large-scale cyber incidents with grave repercussions for millions of affected individuals.[1] The seriousness of this tendency, and in particular the often-concurring information asymmetry between the breached entity on one side and the supervisory authority or affected individuals on the other, was not lost on the legislators. The pioneering act California S.B. 1386 from 2002 initiated the trend towards enforcing greater transparency through data breach notification obligation. This legal framework inspired adoption of similar obligation in all other US-states and also served as basis for more recent similar legal framework in the European Union. Here it was initially limited in scope to the providers of publicly available electronic communications services. This occurred through transposition of the amended Directive on privacy and electronic communications[2] into the national laws of the Member States by mid-2011. Later on, the United States experienced several political endeavours for unified federal-level legislation of the data breach notification. These were mostly sparked by major data breach incidents affecting large portion of the American electorate, as were the cases of Target breach in 2013 or Equifax breach in 2017.

* Ing. Mgr. František Kasl is a Ph.D. student at the Institute of Law and Technology, Faculty of Law, Masaryk University in Brno, Czech Republic

[1] World's Biggest Data Breaches & Hacks. In: *Information is Beautiful* [online]. 1. 2. 2019 [2020-10-02]. Available at: <https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>.

[2] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, OJ 2009 L 337/11. In: EUR-lex.

While these efforts were so far unsuccessful, the European Union adopted the General Data Protection Regulation,[3] which came into force on 25th May 2018 and brought under Art. 33 and 34 data breach notification and communication obligations applicable to all controllers processing the personal data of the 500+ million EU data subjects. This signified a major development in the European personal data protection framework; however, it also continues to pose non-trivial challenges to the numerous controllers, who need to adjust the internal processes, but often lack previous experience or adequate sector-specific guidelines for this obligation. We therefore try to look on the broad and varied experience in the US in an attempt to provide insights and intellectual stimuli for the debate concerning interpretation and application of the notification obligation in the current EU context.

The aim of this paper is not to provide an exhaustive analysis of the US data breach notification legislation, as for such purpose are available numerous existing sources.[4] The introduction to the US regulatory landscape in this contribution is focused on core aspects that can contribute to the debate concerning the similar obligation in the EU. This is supplemented by critical highlight of the limitation of any direct experience transposition between the US and EU personal data protection frameworks, due to inherent conceptual differences.

The contribution is divided into two parts. This part is focused firstly on the questions related to definition of a data breach and its significance in current technological context. The second focal point is then the overview of the main features of the US regulatory framework of the notification obligations. The contribution then continues with part two, which provides insight into the relevant EU provisions and elaborates on the discussion interlocking these two similar normative constructs in related legal systems.

2 WHAT ARE PERSONAL DATA BREACHES AND WHY DO THEY MATTER?

In order to discuss the legislative solutions of data breach notification, it is essential first to establish what constitutes a data breach. The term can be perceived in a broad variety of forms that it can take, which requires focus on definition present in the respective law. However, beyond matter of the legal terminology, there is more essential question to respond to, which is, why does data breach represent an important problem and how is its notification beneficial?

2.1 Occurrence of personal data breach

Personal data breach is a situation often involving a cyber security incident, as these terms are more than partially overlapping. Breach of personal data processing is not lim-

[3] 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 (GDPR). In: EUR-lex.

[4] DAVIS WRIGHT TREMAINE LLP. Summary of U.S. State Data Breach Notification Statutes. In: *Davis Wright Tremaine LLP* [online]. 2019 [2020-10-02]. Available at: <https://www.dwt.com/gcp/state-data-breach-statutes>; STEPTOE & JOHNSON LLP. Comparison of US State and Federal Security Breach Notification Laws. In: *Steptoe* [online]. 2016 [2020-10-02]. Available at: <https://www.steptoe.com/images/content/6/5/v1/6571/Steptoe-DataBreachNotificationChart.pdf>.

ited to incidents in cyberspace; nevertheless, it is the data breaches by electronic means that are currently regarded as the most common and damaging threat.[5] In fact, the increasing frequency and severity of disclosed data breaches has established them as a common aspect to be calculated in costs of doing business.[6] This highlights that personal data breaches became such a frequented phenomenon, that notwithstanding the occasional massive incidents, they are often regarded as a standard feature of enterprise in modern digitalized society. This development is particularly distressing from the perspective of the affected individuals, i.e. the data subjects.

2.1.1 Data breach as a form of cyber security incident

Cyber security incident is a term from cyber security field, focusing on the technical parameters of the event. The main feature of a cyber security incident is the unauthorized or unintended compromise of the ICT system, data or network.[7] The term personal data breach on the other hand relates to the protection of individual's informational self-determination. It takes into account the quality of the compromised data rather than the form of the incident. Therefore, personal data breach may occur also in non-electronic form, if such incident affects documents containing personal data. Nevertheless, in nowadays digitalized economy, the cyber security incident represents the predominant form of personal data breach and current technological trends strongly suggest only increase of their relevance in the future.[8]

2.1.2 Origins of data breach

Personal data breach does in general take a form of either an accident or an unauthorized action. In both cases, the constituting factor is that the situation leads to unintended (from the perspective of the processor, controller and data subject) processing of the personal data. The data may be modified, disclosed, erased, copied or in another way used. The predominance of electronic personal data processing in current society invites a closer look at the most common personal data breaches that take a form of a cyber security incident.

One such spectrum of frequent forms provides the security pattern qualification used by Verizon since 2014. It includes exploits of code-level vulnerabilities in the application; thwarting authentication mechanisms; remote intrusions into point of sale terminals; unapproved or malicious actions of insiders or partners with access privileges; actions of state-affiliated actors; payment card skimmers; denial of service attacks; unintentional actions, like sending data to a wrong recipient or misconfigurations of databases; and

[5] ARTICLE 29 DATA PROTECTION WORKING PARTY. Guidelines on Personal data breach notification under Regulation 2016/679 18/EN WP250rev.01. In: *European Commission* [online]. 6. 2. 2018 [2020-10-02]. p. 7. Available at: <https://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49827>.

[6] MURRAY, T. 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, Vol. 94, No. 1, p. 128.

[7] INTERNATIONAL TELECOMMUNICATION UNION. Definition of cybersecurity. In: *ITU* [online]. 29. 9. 2017 [2020-10-02]. Available at: <http://www.itu.int:80/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx>.

[8] FIGUEROA, Z. Time to Rethink Cybersecurity Reform: The OPM Data Breach and the Case for Centralized Cybersecurity Infrastructure. *The Catholic University Journal of Law & Technology*. 2016, Vol. 24, No. 2, pp. 438–439.

most significantly, all forms of malicious software, primarily used opportunistically with financial motivation, as exemplified by the prevalence of ransomware.[9] Highly relevant are also the unauthorized accesses to personal data through the use of social engineering techniques, which achieve data breach through misleading or manipulation of the human target rather than technical means.[10]

The frequency and impact of identified data breach incidents is staggering. The IBM Security report 2020 counts over 8.5 billion records exposed in this way in 2019 only.[11] To put the scope in another perspective, the Thales report 2020 highlights that 26% of its respondents experienced data breach in the past year.[12] Even so, the picture painted by any available reports is still probably understating the size of the real problem, as there are likely numerous incidents going unreported.[13] Furthermore, even in case of the reported incidents, organizations are mostly sensitive about sharing the data on its details, like the number of records compromised, leaving the true impact of the data breach often blurry.[14]

2.1.3 Harm caused by data breach

The brief summary above of an otherwise rather complex landscape of cyber security incidents affecting personal data should provide the reader with basic overview of the usual situation, in which the stored or processed personal data escapes from the control of the data controller or processor and may be misused by a third party to a detriment of the affected individual.

Such misuse may reach different scale of harm. This can be well demonstrated on the consequences of the Ashley Madison data breach from July 2015.[15] It concerned a data leak of personal information (names, addresses, passwords, payment and credit card details, search history, or preferences) about users of this commercial website for extra-marital affairs. The mere public availability of such sensitive information infringed upon privacy and dignity of the identified adulterers and was likely to have negative impact on their marital, social or work relationships. Such information could be further used for manipulation of the persons, or extortion. Blackmailing was present also in case of Ashley Madison data breach, in particular towards victims with .sa (adultery is a crime in Saudi Arabia) or .mil (military personnel) and .gov (U.S. governmental employees) e-mail ad-

[9] VERIZON. 2019 Data Breach Investigations Report. In: *Verizon* [online]. 2019 [2020-10-02]. p. 23. Available at: <https://enterprise.verizon.com/resources/reports/dbir/>.

[10] HADNAGY, CH. *Social engineering The Art of Human Hacking*. Indianapolis: Wiley Publishing, 2011, ISBN: 978-0-470-63953-5, p. 3; MOUTON, F., LEENEN, L., VENTER, H. Social engineering attack examples, templates and scenarios. *Computers & Security*. June 2016, Vol. 59, pp. 187 et seq.

[11] IBM X-FORCE INCIDENT RESPONSE AND INTELLIGENCE SERVICES. X-Force Threat Intelligence Index 2020. In: *IBM* [online]. 2020 [2020-10-02]. p. 8. Available at: <https://www.ibm.com/downloads/cas/DEDOLR3W>.

[12] IDC. The Changing Face of Data Security 2020 Thales Data Threat Report Global Edition Thales. p. 7. In: *Thales Security* [online]. 2020 [2020-10-02]. Available at: <https://www.thalesesecurity.com/sites/default/files/2020-02/2020-data-threat-report-global-edition-report.pdf>.

[13] BISOGNI, F., ASGHARI, H., VAN EETEN, M. Estimating the size of the iceberg from its tip. In: *16th Annual Workshop on the Economics of Information Security*. *WEIS 2017*. San Diego: University of California, 2017.

[14] RISK BASED SECURITY. Data Breach QuickView Report 2019 Q3 Trends p. 10. In: *Risk BAsed Security* [online]. 2019 [2020-10-02] Available at: <https://pages.riskbasedsecurity.com/data-breach-quickview-report-2019-q3-trends>.

[15] MANSFIELD-DEVINE, S. The Ashley Madison affair. *Network Security*. 2015, Vol. 2015, No. 9, pp. 8 et seq.

dresses.[16] As another example, the access to passwords and credentials to e-mail or other online accounts would allow for an identity theft.[17] This criminal activity is a form of fraud, where the perpetrator takes over the virtual identity of the victim through administration of their accounts on social media, e-mail, online marketplaces or internet banking platforms and acts without authorization in their name and on their account to their detriment. This leads to major impact on the individual, i.e. through damage to his reputation, disclosure of his private communication, psychological and emotional distress due to loss of control, possible financial loss or need to abandon the account and all its personalized content to start anew and regain control.

Many data breach cases involve merely a risk of such abuse or takeover of one's virtual identity, which do not have to materialize.

The overall trend of digital transformation brings new cyber security concerns, along with more frequent incidence of hacking into business databases and increasing severity and size of reported data breaches.[18] Aside from impact on the affected individuals the personal data breach also leads to direct and indirect cost implications for the business entity. It triggers possible reputation damage, media scrutiny, loss of customers, increased cash flow risks, as well as regulatory sanctions or litigation and settlement expenses.[19]

2.2 Legal definition of personal data breach

The term "personal data breach" (or "security breach", as used in the US law[20]) is part of various legal norms focused on protection of personal data. However, the frequent diversity in the use of underlying term "personal data" (also "personal information" or "personally identifiable information", as used in the US law) leads to varying scope of events that in the end constitute a personal data breach. The differences can be found not only between the US and EU legislative approaches, but also within both of these areas of legal tradition.

2.2.1 US legislation

The lack of single definition of data breach in the US legislation is obvious consequence of the fragmented approach to the regulation of personal data protection and data breach notification.[21] This shall be described in detail in a later section; however, the lack of gen-

[16] FRANCE 24. The global fallout of the Ashley Madison hack. In: *France 24* [online]. 2015 [2020-10-02]. Available at: <https://www.france24.com/en/20150820-global-fall-out-ashley-madison-hack>.

[17] LAI, F., LI, D., HSIEH, CH. Fighting identity theft: The coping perspective. *Decision Support Systems*. 2012, Vol. 52, No. 2, pp. 353 et seq.

[18] IBM X-FORCE INCIDENT RESPONSE AND INTELLIGENCE SERVICES. *X-Force Threat Intelligence Index 2020* p. 5. [online]. IDC. *The Changing Face of Data Security 2020 Thales Data Threat Report Global Edition* p. 23.

[19] KAMIYA, S. et al. What is the Impact of Successful Cyberattacks on Target Firms? *National Bureau of Economic Research: Working Papers* No. 24409. [online]. 2018 [2020-10-02]. Available at: <https://www.nber.org/papers/w24409>.

[20] DE BRUYNE, M. F. *Data breach notification and the risk of over-notification under the GDPR. A comparative analysis of US and EU experiences in practice*. Master's Thesis Tilburg: Tilburg University. p. 9. [online]. 5. 6. 2016 [2020-10-02]. Available at: <http://arno.uvt.nl/show.cgi?fid=140479>.

[21] MURRAY, T. 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, Vol. 94, No. 1, p. 136.

eral federal legislation and piecemeal adoption of state statutes created a disharmonious array of similar-but-not-same definitions of data breach. *Murray* points out the lack of unified definition in the statutes by the example of comparison between Michigan and Ohio statutes. Both involve in their definition unauthorized access and acquisition of data that compromises the security or confidentiality of personal information. However, Ohio further requires a reasonable belief that such access and acquisition caused, or will cause, a material risk of harm.[22] Possibly the most influential definition of data breach provided the original California statute, as it served as example to many later adoptions of similar statutes in other US-states. It provides suitably flexible and broad definition: *"A "breach of the security of the system" is the "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business."*[23] An exception from the definition is provided for "*good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business […], provided that the personal information is not used or subject to further unauthorized disclosure.*"[24] As such, the California statute does not incorporate the necessity for determination of risk of harm, as does the above described Ohio statute. This is in fact often a core modification that many statutes adopted in comparison to the California definition.[25] Another restriction to the term often present in the US-state statutes is the limitation to unauthorized acquisition of unencrypted computerized data without parallel disclosure of the key to the encryption.[26] Over the past decade, the negative impact of fragmentation of the data breach legislation on the US state-level was recognized by the federal legislator and several attempts with noteworthy public support were made towards general federal statute concerning personal data breach notification. The most significant attempt for uniform US standard for data breach notification was the 2015 proposed Personal Data Notification and Protection Act. Here the approach was similarly broad as in the California statute. However, as of now, there is no successfully adopted version of the federal law concerning data breach notification. The US law definition therefore remains fragmented and sector- and jurisdiction-dependent.

2.2.2 EU legislation

The European experience with personal data breach notification legislation was until recently limited to obligations for providers of publicly available electronic communications services.[27,28] The major shift was brought on 25th May 2018 by coming into force of

[22] Ibid. p. 130.
[23] California Civil Code (2017) Section 1798.82 (g).
[24] Ibid.
[25] E.g. Maine Revised Statute (2009), Title 10 Chapter 210-B, Section 1348 (1); Louisiana Revised Statute 51 (2011), Section 3074 (G); Kansas Statute (2006), Section 50 - 7a02 (a); Iowa Statute Title 16 Chapter 715C (2017), Section 2 (6); Florida Statute Chapter 501 (2014) Section 501.171(4)(c).
[26] E.g. Kentucky Revised Statute Chapter 365 (2014), Section 365.732(1)(a); Rhode Island General Laws Title 11 (2012), Section 49.2-5(b); Tennessee Code Title 47 (2010), Section 2107(a)(1).
[27] Directive 2009/136/EC.
[28] Sector-specific variations of breach notification obligation are further present in the Art. 14 and 16 of the NIS Directive 2016/1148, Art. 96 of the PSD2 Directive 2015/2366 and the Art. 19 of the eIDAS Regulation 910/2014.

the General data protection regulation 2016/679 (widely known under its acronym as "GDPR"),[29] which introduced obligation to notify personal data breaches to all data controllers. This shift was anticipated throughout the long preparation stage and intermediary stage after adoption. The Netherlands even adopted in the meantime specific national law that entered into force on 1st January 2016 and introduced the data breach notification obligation before GDPR.[30] Similar bridging provision was introduced in 2017 into the German national legislation.[31] The terminology in the EU is due to this development practically unified, as the GDPR adopted the definition previously implemented through the Directive 2009/136/EC for providers of publicly available electronic communications services. A personal data breach is thereby defined as *"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."*[32] The underlying concept of personal data is also understood broadly 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*".[33] There are no explicit exceptions to the EU definition of personal data breach and there is no necessity for determination of risk of harm as is many US statutes. However, the exceptions, similarly as in some US statutes, are often implicit, depending on proportionality assessment of various elements, including the risk for affected data subjects or level of encryption adopted.[34]

2.2.3 Definition applicable to this contribution

Despite the above noted divergence in the formulation of the definition, the terms in US and EU legislation are mostly covering similar incidents. The core similarities are given by the compatible aim of the respective notification obligations in both systems, as shall be further elaborated throughout both parts of this contribution. However, the variations in the scope and terminology across US statutes needs to be kept in mind, as it affects the scope of notification obligation and modifies its specific parameters. There are four core aspects that have this impact, which may lead to limited transposition of the US experience to the EU setting.

[29] 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 (GDPR). In: EUR-lex.

[30] DE BRUYNE, M. F. *Data breach notification and the risk of over-notification under the GDPR. A comparative analysis of US and EU experiences in practice.* Master's Thesis Tilburg: Tilburg University. p. 51. [online]. 5. 6. 2016 [2020-10-02]. Available at: <http://arno.uvt.nl/show.cgi?fid=140479>.

[31] Section 42a Bundesdatenschuztgesetz, BGBL, 2017, Part I No. 2097.

[32] Art. 4 no. 12 GDPR.

[33] Art. 4 no. 1 GDPR.

[34] ARTICLE 29 DATA PROTECTION WORKING PARTY. *Guidelines on Personal data breach notification under Regulation 2016/679 18/EN WP250rev.01*.

First and foremost, it is the different concept of the protected personal data. The EU data protection framework has particularly broad understanding of personal data.[35] The US statutes on the other hand mostly focus on a rather limited set of data that directly identify a natural person and can be perceived as sensitive or allow for direct misuse leading to quantifiable damage to the affected person.[36] This difference is reflection of the different foundations of the personal data protection in these jurisdictions.[37] Nevertheless, as the scope is broader in the EU setting, the obstacle this poses for the conclusions can be largely overcome by adopting the logical *a minori ad maius* argumentation, i.e. through focusing on the core of EU data breach notification regulation, which is similar to US setting, while accepting the presence of additional border areas in the EU law that are incomparable with the US experience.

The second difference can be seen in the concept of personal data breach itself. Whereas in EU the acquisition of the affected personal data is only one of the forms of the breach, standing beside destruction, loss, or alteration, in the US it is often the whole scope of the term.[38] Even here though the limited discussion based on *a minori ad maius* argumentation remains similarly applicable.

From the perspective of many US state statutes, the occurrence of personal data breach is further precluded by the use of (secure) encryption or the insufficiently determined likelihood of risk of harm (meaning lack of provable quantifiable damage caused to the data subject in consequence of the data breach). In the EU perspective, the encryption serves merely as a technical measure mitigating the resulting risk, but does not declassify the incident as personal data breach. Similarly, the necessity of the risk of harm prerequisite is excluded by the quality of personal data protection as fundamental right pursuant to the Article 8 of Charter of Fundamental Rights of the European Union. The mere violation of this right through the data breach is therefore sufficient to constitute the legally relevant event and the provable quantifiable damage caused then merely supports the evidence of detriment related to it.

The US statutes, notwithstanding the particularities, provide the entities processing personal data with narrower obligations with regard to personal data breach than the GDPR, as the mere understanding of what constitutes a personal data breach is much broader in the EU. This is related to the more general lack of comprehensive privacy and data protection regulation in the US.[39] This means that the insights for the US settings cannot be directly linked to the new EU framework. On the other hand, if there are challenges identified with compliance to the narrow obligations in the US, it can be assumed,

[35] KOOPS, B.-J. The trouble with European data protection law. *International Data Privacy Law*. 2014, Vol. 4, No. 4, pp. 250 et seq.

[36] BURDON, M. Contextualizing the Tensions and Weaknesses of Information Privacy and Data Breach Notification Laws. *Santa Clara Computer & High Tech. L. J.* 2010, Vol. 27, No. 1, p. 86.

[37] SCHWARTZ, P., PEIFER, K.-N. Transatlantic Data Privacy Law. *The Georgetown Law Journal*. 2017, Vol. 106, No. 1, pp. 121 et seq.

[38] MURRAY, T. 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, Vol. 94, No. 1, p. 130.

[39] RAUL, C.; AUSTIN, S. (eds.) *Chambers Global Practice Guide: Data Protection & Cyber Security 2019*. Glasgow: Chambers & Partners, 2018, ISBN: 978-0-85514-746-4, pp. 368–369.

that similar or more daunting challenges are likely to be present when facing the broader and more complex obligations in the EU.

In face of these limitations, this contribution shall adopt as relevant the basic version of personal data breach definition provided in the US law modified with standard EU law terminology, i.e. data breach shall be primarily understood as an unauthorized acquisition of personal data that compromises their confidentiality, integrity or availability, excluding certain good faith acquisitions.

3 THE MAIN SPECIFICS OF THE US LAW RELEVANT TO THIS CONTRIBUTION

Despite historical predominance of case law as the primary component of the US law, the nowadays system is much closer to a mixed system. Through increasing role of statutes and codifications the US law is coming closer to meet with the Continental European legal systems, which on the other hand add growing importance to decisional law.[40]

The legislation is divided into state law and federal law, whereas state law is by no means uniform. The US-states are independent legal systems with separate trees of judiciary, as there is no superior judicial authority to unify the divergent state practices on the federal level.[41] Crucial for interpretation of the US law remain the legal precedents, pursuant to the established doctrine of stare decisis. The US-state law is interpreted separately for each state through its own branch of judiciary crowned by a State Supreme Court.[42] Navigating the landscape of the US-state case law for research outside of the US was largely made possible thanks to its inclusion into the Google Scholar database.[43] The US procedural law for civil lawsuits has numerous particularities, of which relevant for this contribution are the possibility of punitive damages[44] and the procedural device of class action.[45]

There is no comprehensive US legal framework for protection of privacy or data security, let alone personal data protection.[46] As presented in detail by *Schwartz* and *Peifer,*[47] the theoretical concept of privacy under the US law is in key aspects divergent from the European understanding of privacy. Under the US law, privacy is not dissimilar to commodity that is evaluated by the individual as consumer in the free and open market and protection of privacy is primarily based on fair conditions for such choice.[48] This deeply

[40] HAY, P. *Law of the United States*. München: C.H.Beck, 2005, p. 7.
[41] Ibid. pp. 8–9.
[42] Ibid. p. 9.
[43] STANLEY, T. Free US Case Law from Google! – US Federal + 50 State Case Law. In: *Justia Law Blog* [online]. 17. 11. 2009 [2020-10-02]. Available at: <https://lawblog.justia.com/2009/11/17/free-us-case-law-from-google-us-federal-50-state-case-law/>.
[44] Damages aimed at punishing the defendant and deterring others. They link to the financial capacity of the defendant not the harm done to the plaintiff. See HAY, P. *Law of the United States*. München: C.H.Beck, 2005, pp. 69 and 174–175.
[45] Ibid. pp. 78–79.
[46] RAUL, C.; AUSTIN, S. (eds.) *Chambers Global Practice Guide: Data Protection & Cyber Security 2019*. Glasgow: Chambers & Partners, 2018, ISBN: 978-0-85514-746-4, p. 359.
[47] SCHWARTZ, P., PEIFER, K.-N. Transatlantic Data Privacy Law. *The Georgetown Law Journal*. 2017, Vol. 106, No. 1, p. 106.
[48] Ibid. p. 121.

entrenched consumer protection and free marketplace perspective is in stark contrast to the European perception of privacy. Here it is seen as an intrinsic human value and fundamental right to informational self-determination.[49]

Following from this rift in value attribution, the available legal devices for personal data protection in the US are closely linked to consumer protection. The core of this is the unfair trade law and authority of the Federal Trade Commission (FTC) to the definition of what constitutes a prohibited unfair and deceptive acts or practices (UDAP).[50] Despite this indirect link, it allowed the FTC to act as *de facto* regulator for the issues of privacy and data security,[51] which include the notification obligations discussed in this contribution. This link to consumer protection may also explain the early emergence of the data breach notification obligation legislation, as a support tool for more effective class actions in case of provable damage caused by inadequate protective measures on part of the data processing entity.

The EU perspective is on the other hand more focused on overall creation of data protection environment build on principles and balancing acts that imbue the consideration of the impact of each business decision on the data subjects into the deep fabric of everyday doing business.[52]

These broader disparities notwithstanding there still remains considerable overlap between the purpose, scope and tools of personal data protection legislation in the US and the EU; in particular concerning the data breach notification. The aim of the obligations is focused overall on transparency and mitigation of potential damage through elevation of the information asymmetry about the detrimental event. As such, it is to a large degree challenged with similar issues, such as disbalance of incentives for compliance on part of the obliged entity.

4 US DATA BREACH NOTIFICATION LEGISLATION

The legal framework of data breach notification in the United States is a combination of state-level privacy and data protection regulation and of specific federal regulation tackling the risks of large-scale operations with sensitive personal data, typical for financial or medical sector.

It was initially in the financial sector, through the authorization of the regulatory authorities to broaden obligations under data protection procedures pursuant to the Gramm-Leach-Bliley Act from 1999,[53] that the concept of notifying the affected parties about the data breach in order to mitigate the arisen or looming damage took hold.

[49] Ibid. p. 123.
[50] HAY, P. *Law of the United States*. p. 278.
[51] RAUL, C.; AUSTIN, S. (eds.) *Chambers Global Practice Guide: Data Protection & Cyber Security 2019*. p. 359.
[52] EUROPEAN COMMISSION. *Communication from the Commission to the European Parliament and the Council: Data protection rules as a trust-enabler in the EU and beyond – taking stock. COM(2019) 374 final*. 2019, p. 1. In: EUR-lex.
[53] Gramm–Leach–Bliley Act (1999), Public Law 106–102, 113 Stat. 1338.

However, first genuine legislative stipulation of data breach notification came in the year 2002 with the enactment of the bill California S.B. 1386, also known as California Security Breach Information Act. This state level legislation was a reaction to increasing impact of data breach events and growing urgency to provide the affected individuals with adequate early warning mechanism and decrease the risk of identity theft.

Since the passage of the California law, all the other 49 states have passed similar laws.[54] Partial reason for this widespread adoption of data breach notification provisions in state-level legislation remains the repeatedly unsuccessful progress towards enactment of unified federal-level obligation that could mitigate some of the significant weaknesses of current regulatory framework of data breach notification in the United States, most notably the fragmented and labyrinthine maze of similar, but non-harmonized state-level statutes.

This section aims to provide a brief summary of the main features of US legal framework of personal data breach in its many iterations and offer a basis for the later comparison with the EU law and discussion of transferable experiences between these frameworks in the second part to this contribution.

4.1 California statute

The Security Breach Information Act was proposed by California State Assembly Member Joe Simitian and California State Senator Stephen Peace on 12th February 2002,[55] largely in reaction to recent major data breach of the Stephen P. Teale Data Centre, which compromised personal information of 265,000 California state employees.[56] It came into force on 1st July 2003 as an amendment to the California Civil Code §§ 56.06, 1785.11.2, 1798.29 and 1798.82.

The progressive nature of this statute made it into a model for numerous further reiterations of data breach notification law in other US states, even though the minor differences in scope or definitions consequentially lead to fragmentation and complex picture on the US-wide scale. In order to be able to discuss these various state-level provisions, a set of comparable core aspects needs to be identified that derive from the aim and structure of the legal instrument of data breach notification. In order to assess the scope of the notification obligation, three parameters are taken into consideration: the definition of covered data, the definition of the data breach event and the scope of entities obligated to notify. In order to assess the form of the notification, it is further taken into consideration, if the notification shall be towards affected data subjects or supervisory authority. Further aspects to consider are the timeframe for notification, the possible exceptions or threshold and the sanctions or private right of action available in case of non-compliance.

---

[54] BOASIAKO, K. A., O'CONNOR KEEFE, M. The Consequences of Data Breach Disclosure Laws and Disclosed Breaches on Corporate Cash Holdings and Performance. In: *SSRN Electronic Journal* pp. 1–2. [online]. 2018 [2020-10-02]. Available at: <https://www.ssrn.com/abstract=3191692>.

[55] SIMITIAN, J., PEACE, S. *SB 1386 Senate Bill*. 2002. [online]. [2020-10-02]. Available at: <leginfo.ca.gov>.

[56] SAMUELSON LAW, TECHNOLOGY & PUBLIC POLICY CLINIC. *Security Breach Notification Laws: Views from Chief Security Officers* Berkley: University of California-Berkeley School of Law. p. 8. [online]. 2007 [2020-10-02]. Available at: <https://www.law.berkeley.edu/files/cso_study.pdf>.

The California statute applies to personal information, with the exception of data made lawfully available from public administration records.[57] Personal information as such is defined either as an unencrypted combination of name and listed categories of sensitive data (especially social security number, driver's licence number, account number, password to online banking, medical information or health insurance information) or as access credentials to online account (e.g. user name and password).[58] As such, the definition can be perceived even from European perspective as reasonably broad, encompassing major categories of data than can be misused to the detriment of the identified person.

The definition of data breach in the California statute was already discussed in a previous section of this paper, however, the main feature to be emphasized is the absence of the prerequisite in the form of provable quantifiable damage caused to the affected person.

The structure of obliged entities resembles the European roles of data controller and processor. As such, person or entity conducting business in California and owning or licencing computerized data including personal information is subject to the notification obligation.[59] Person or entity maintaining such data shall inform the owner or licensee about the data breach immediately following its discovery.[60] The exceptions apply to entities subject to sector-specific federal legislation (i.e. health care providers and financial institutions).[61]

The notification obligation includes both communication to the data subject and notification to public authority.[62] The threshold for communication to the affected residents of California is set low to a level of reasonable belief of unencrypted personal information been acquired by an unauthorized person.[63] The notification is to be made to California Attorney General, which established a specialized Privacy Enforcement & Protection Unit replacing the formerly separate California Office of Privacy Protection,[64] in case of data breach affecting more than 500 residents, whereas the notification shall take the form of a sample of the distributed notice.[65] The given thresholds indicate the priority of communication towards affected parties over public authority.

The communication shall follow the discovery of the data breach in the most expedient time possible and without unreasonable delay;[66] the formerly recommended indicative timeframe was 10 business days.[67] Nevertheless, the statute provides for exception in case

[57] California Civil Code (2017), Section 1798.80 (e).
[58] California Civil Code (2017), Section 1798.82 (h).
[59] California Civil Code (2017), Section 1798.82 (a).
[60] California Civil Code (2017), Section 1798.82 (b).
[61] California Civil Code (2017), Section 1798.82 (e).
[62] The terminology of "communication" towards data subject and "notification" towards supervisory authority is used in GDPR in respective Art. 33 and 34 and as such is chosen as default for the purpose of this contribution for the benefit of the primarily European target audience.
[63] California Civil Code (2017), Section 1798.82 (a).
[64] OFFICE OF THE ATTORNEY GENERAL. Privacy Enforcement and Protection. *State of California Department of Justice* [online]. 11. 10. 2012 [2020-10-02]. Available at: <https://www.oag.ca.gov/privacy>.
[65] California Civil Code (2017), Section 1798.82 (f).
[66] California Civil Code (2017), Section 1798.82 (a).
[67] CALIFORNIA OFFICE OF PRIVACY PROTECTION. *Recommended Practices on Notice of Security Breach Involving Personal Information* p. 12. [online]. 2012 [2020-10-02]. Available at: <https://bcourses.berkeley.edu/courses/1463120/files/71435731/download?verifier=b6heYnAye5G7U34dAxoiRw7iSzcRwYOv6lWKfxC5&wrap=1>.

of legitimate needs for delay on the side of law enforcement, or, more importantly, excludes the time needed for any measures necessary for determination of the scope of the breach and restoration of reasonable integrity of the data system.[68] The regulation is furthermore more lenient towards businesses with customized notification procedures as part of information security policy.[69] Business failing to comply with the obligation may be enjoined[70] as well as subject to private civil action to recover damages by any injured customer.[71] Waiver of this right is void and unenforceable.[72]

4.2 Statutes in other US states

The scope of the definition of personal data (more precisely personally identifiable information in the US legal terminology) across US-state jurisdictions varies, however, the basic scope common throughout the jurisdictions includes either name combined with unencrypted Social Security number, driver's licence or state ID number; or financial information like account number or credit card number together with respective access code or password. Apart from that, multiple statutes broaden the scope to other forms of sensitive personal data, for example: Wisconsin statute[73] includes DNA profile and biometric data; Northern Dakota statute[74] specifically mentions electronic signatures, date of birth, as well as maiden name of the resident's mother; Florida[75] code applies also broader to user name or e-mail address combined with password or security answer for personalised online account; in comparison Wyoming stature[76] includes shared secrets and security tokens used for data based authentication.

Most US statutes are applicable only to data breaches concerning electronically processed personal data. The exceptions can be found in Washington,[77] Alaska,[78] Wisconsin,[79] Iowa,[80] Indiana,[81] Massachusetts,[82] North Carolina[83] and Hawaii.[84]

The base definition of data breach event as such is largely homogenous throughout the US. It is mostly defined as unauthorized acquisition of entity's data that compromises the security, confidentiality, or integrity of the contained personal information, with the ex-

[68] California Civil Code (2017), Section 1798.82 (a).
[69] California Civil Code (2017), Section 1798.82 (k).
[70] California Civil Code (2017), Section 1798.84 (e).
[71] California Civil Code (2017), Section 1798.84 (b).
[72] California Civil Code (2017), Section 1798.84 (a).
[73] Wisconsin Statutes Chapter 134 (2007), Section 134.98.
[74] North Dakota Century Code (2017), Section 51-30-01 et seq.
[75] Florida Statute Chapter 501 (2014), Section 501.171.
[76] Wyoming Statues Title 40 Chapter 12 (2018), Section 501-502.
[77] Washington Statute Title 19 Chapter 255 (2015), Section 010-020.
[78] Alaska Statute Title 45 Chapter 48 (2018), Section 010.
[79] Wisconsin Statutes Chapter 134 (2007), Section 98.
[80] Iowa Statute Title 16 Chapter 715C (2017), Section 1 and 2.
[81] Indiana Code Title 24 Article 4.9 (2017), Section 1 et seq.
[82] Massachusetts General Law Part I Title XV Chapter 93H (2019), Section 1-6.
[83] North Carolina Statute (2015), Section 75-61 and 75-65.
[84] Hawaii Revised Statute (2019), Section 487N-1 et seq.

clusion of certain described cases of good faith acquisition. Nevertheless, even in this regard may be found some minor derivations, for example the Ohio statute does not include the consideration of integrity breach,[85] or the Florida statute, which makes do with simplified definition as "unauthorized access of data in electronic form containing personal information."[86]

The major divide throughout the US statutes is regarding the incorporation of harm prerequisite into the definition of the obligation. California is an example of jurisdiction with low threshold standard, similar situation is in Nevada,[87] Texas,[88] Georgia,[89] New York[90] and several other jurisdictions. Most other jurisdiction, for example Ohio, Florida, Wyoming or Iowa, however follow the heightened threshold, conditioning the notification obligation on the occurrence of reasonable risk of harm to the identified individuals.

The statutes further mildly differ in formulations considering the relevance of (secure) encryption and potential safe harbour from notification obligation pursuant to this protective measure, mostly however follow the suit set by the California statute.

Further fragmentation occurs with regard to the prescribed recipient of the notification. Several statutes, among them those of Idaho,[91] Utah,[92] or Mississippi,[93] limit the notification obligation to communication of the data breach towards the affected individuals. However, the trend is towards incorporating the state authorities at least regarding large data breaches, as can be seen for example from the development in Arizona.[94] The most common public recipient is the state Attorney General, pursuant to the example of California. Puerto Rico notifications shall be directed towards local Department of Consumer Affairs,[95] whereas in Arkansas only some entities are obliged to report breaches to Securities Commissioner or Insurance Commissioner.[96] On the other hand, multiple states opt instead for notification of large data breaches towards the state consumer representation agency, as is the case in Kansas[97] and Pennsylvania[98] for breaches affecting over 1000 residents, or in Texas[99] and Georgia,[100] if over 10 000 residents are affected. In a number of states is then the situation more complex, as the notification is required towards the state

[85] Ohio Revised Code Title 13 Chapter 1349 (2007), Section 1349.19(A)(1)(a).
[86] Florida Statute Chapter 501 (2014), Section 501.171(1)(a).
[87] Nevada Revised Statute Chapter 603A (2017), Section 010 et seq.
[88] Texas Business and Commerce Code Chapter 521 (2009), Section 002, 053 and 151.
[89] Code of Georgia Title 10 Chapter 1 (2019), Section 910 et seq.
[90] The Laws of New York General Business Article 39-F (2019), Section 899-AA.
[91] Idaho Statute Title 28 Chapter 51 (2014), Section 104 et seq.
[92] Utah Code Title 13 Chapter 44 (2010), Section 101 et seq.
[93] Mississippi Code Title 75 Chapter 24 (2019), Section 29.
[94] ARIZONA ATTORNEY GENERAL. New Arizona Law to Protect Data Breach Victims. *Arizona Attorney General Mark Brnovich* [online]. 2019 [2020-10-02]. Available at: <https://www.azag.gov/press-release/new-arizona-law-protect-data-breach-victims>.
[95] Laws of Puerto Rico Title TEN (2019), Section 4051-4055.
[96] Arkansas Code Title 4 Chapter 110 (2019), Section 101 et seq.
[97] Kansas Statute (2006), Section 50-7a01-04.
[98] Pennsylvania Statutes Title 73 Chapter 43 (2006), Sections 2301-2308 and 2329.
[99] Texas Business and Commerce Code Chapter 521 (2009), Sections 002, 053 and 151.
[100] Code of Georgia Title 10 Chapter 1 (2019), Section 910 et seq.

Attorney General as well as state consumer representation agency. This is the case for example in Florida,[101] North Carolina,[102] Maine,[103] or Montana.[104]

The timeframe set for notification is very consistently set by the flexible formulation of "without unreasonable delay", however some statutes additionally set maximal deadlines to strengthen the obligation and promote higher level of protection of the affected individuals. For example, the Delaware statute prescribes the maximal timeframe to 60 days after the determination of the data breach,[105] Ohio,[106] Washington[107] or Oregon[108] statutes operate with 45-day threshold, whereas Florida statute sets it to 30 days.[109]

Private remedies are a standard feature throughout the US-state statutes, supported by the established framework for civil class actions. Unspecified civil penalties support compliance with most state-level statutes. Additionally, some states provide for specific statutory penalties, as for example Hawaii ($2 500 per violation),[110] or Texas (between $2 000 and $50 000 per violation).[111] The statutory penalty in the Florida statute is graded following the period of non-compliance.[112] The Washington statute specifically states that failure to notify is to be deemed as an unfair or deceptive act in trade or commerce or unfair method of competition for purposes of consumer protection.[113]

Overall, this provides for a complex mesh of similar-but-not-the-same regulatory regimes, where it is difficult to identify the most or the least strict regime overall, as most provide stricter setting in one aspect, but looser requirements in another.

4.3 Case law and Attorney General activity regarding data breaches

In US legal tradition, the dominant role in interpreting and adapting the law to the heartbeat of the society falls to the case law. The occurrence of data breach has mostly negative impact on the affected individuals, thereby establishing a likely basis for a lawsuit or even a class action, given the usual multitude of adversely affected individuals. Private litigation is well established tradition in the US legal system. However, the fragmented nature of data breach legislation and data protection law in general means that the plaintiffs approach the harm caused by data breach from multitude of directions. The lawsuits are therefore based on diverse claims ranging from breach of contract, breach of duty or misrepresentation through breach of good faith or breach of warranty to specific grounds for statutory damages following from federal as well as state-level

[101] Florida Statute Chapter 501 (2014), Section 171.
[102] North Carolina Statute (2015), Section 75-61 and 75-65.
[103] Maine Revised Statute Title 10 Chapter 210-B (2009), Section 1346-1350-B.
[104] Montana Code Title 30 Chapter 14 Part 17 (2017), Sections 1704 and 1705.
[105] Delaware Code Title 6 Chapter 12B (2017), Section 101 et seq.
[106] Ohio Revised Code Title 13 Chapter 1349 (2007), Sections 19, 191 and 192.
[107] Washington Statute Title 19 Chapter 255 (2015), Section 010-020.
[108] Oregon Revised Statute Chapter 646A (2018), Sections 600-604 and 624-626.
[109] Florida Statute Chapter 501 (2014), Section 171.
[110] Hawaii Revised Statute (2019), Section 487N-1 et. seq.
[111] Texas Business and Commerce Code Chapter 521 (2009), Sections 002, 053 and 151.
[112] Florida Statute Chapter 501 (2014), Section 171.
[113] Washington Statute Title 19 Chapter 255 (2015), Section 010-020.

statutes.[114] This reflects the sheer versatility of data breach situations and difficulty of tackling this phenomenon within the established US private law framework.

Furthermore, the development of the various state jurisprudence regarding key aspects of such claims, such as the recognizable harm caused by the data breach, is quite inconsistent and until recently prioritized dismissal of harm recognition in case no injury in fact was proved.[115] The failure to establish harm in private actions following on a data breach has two major impacts.

Firstly, despite US-state only data breach notification legislation, the cases concerning data breach often end up being heard in front of the federal courts, pursuant to the procedural rules of the federal *Class Action Fairness Act*.[116] In this procedural setting, failure to establish harm leads to loss of standing and dismissal of the case.[117]

Secondly, if plaintiffs in private litigation fail to prove harm, the court cannot grant them the case.[118] The 2013 Supreme Court of the United States conclusion in the *Clapper v. Amnesty International* case led to widespread dismissal of data breach cases by US courts on the grounds of lack of provable harm.[119] The data breach as such rarely leads to clearly quantifiable injury as a consequence of the misuse of the accessed personal data. The failure to sue for either increased probability of the potential injury due to the data breach or for anxiety or other intangible harm caused to the affected data subjects through the increased risk to their virtual assets and identities thereby effectively eliminates the private class actions as coercive instrument towards compliance with data breach notification laws.

This development is further supported by empirical data from the 2014 study by *Romanovsky et. al.*,[120] which analysed 230 lawsuits concerning data breaches and established that vast majority (all but two) of the cases terminated before trial, either through dismissal or by settlement.[121] Examples of such settlements include the 50 million USD settlement by Yahoo! for the massive 2014 data breach[122] or 115 million USD settlement by Anthem for major data breach in 2015.[123]

The 2016 Supreme Court of the United States decision in *Spokeo, Inc. v. Robins*[124] opened a leeway for data breach claims through admission of increased risk of intangible injury as permissible form of harm.[125] However, this new perspective failed to provide a clear

[114] ROMANOSKY, S., HOFFMAN, D., ACQUISTI, A. Empirical Analysis of Data Breach Litigation. *Journal of Empirical Legal Studies*. 2014, Vol. 11, No. 1, p. 25 figure 7.
[115] SOLOVE, D., CITRON, D. Risk and Anxiety: A Theory of Data Breach Harms. *Texas Law Review*. 2016, Vol. 2018, No. 96, p. 737.
[116] Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d) (2012).
[117] SOLOVE, D., CITRON, D. Risk and Anxiety: A Theory of Data Breach Harms. *Texas Law Review*. 2016, Vol. 2018, No. 96, p. 750.
[118] Ibid. p. 747.
[119] Ibid. p. 741.
[120] ROMANOSKY, S., HOFFMAN, D., ACQUISTI, A. Empirical Analysis of Data Breach Litigation. *Journal of Empirical Legal Studies*. 2014, Vol. 11, No. 1.
[121] Ibid. p. 92.
[122] Yahoo! Inc. Customer Data Security Breach Litigation, No. 16-2752 (N.D. Cal.) 22. 10. 2018.
[123] Anthem, Inc. Data Breach Litigation, No. 15-2617 (N.D. Cal.) 16. 8. 2018.
[124] U.S. Supreme Court decision Spokeo, Inc. v. Robins, 136 S.Ct. 1540 (2016).
[125] SOLOVE, D., CITRON, D. Risk and Anxiety: A Theory of Data Breach Harms. *Texas Law Review*. 2016, Vol. 2018, No. 96, p. 744.

guidance for data breach cases and the case-law therefore remains patchy.[126] As such the standing in front of the federal courts remained the key issue of data breach cases also in 2018 and settlements remained a frequent occurrence.[127] In consequence, the current state of US data breach case law indicates inefficiencies, caused on one hand by the lack of consistent and comprehensive legal framework for this area in the US law, but on the other hand also the complexity of capturing the impact of the data breach under the applicable standard for prove of harm and thereby limits of private litigation in this direction.

The substitute role for ensuring compensation of the affected individuals, at least in the most damaging and wide-reaching cases of data breach, seems to be taken up by the Attorney Generals. Such were the cases of the 18,5 million USD settlement for the 2013 data breach by Target,[128] the 148 million USD settlement for the 2016 data breach by Uber or the record-breaking 600 million USD settlement for the massive 2017 data breach by Equifax.[129] Therefore, despite the prioritized standing of private litigation in the US legal system, the area of data breaches is gradually transformed into a system closer resembling the EU protection of data subjects through the actions of the data protection authorities. This is even more valid for the sectoral legislation on the federal level.

4.4 Sector-specific federal laws

The main two areas subordinated under specific legal regime with regard to data breach notification requirements in the US are financial and medical sector data.

The legal basis for data processed by financial institutions can be found in the Gramm-Leach-Bliley Act.[130] Pursuant to Section 501(a), the relevant regulatory authorities shall establish appropriate standards of administrative, technical, and physical safeguards for security of the customer records and information and in order to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer. The regulation is applicable to financial institutions encompassing banks as well as other financial non-banking entities. The group of US bank regulatory agencies issued in 2001 Interagency Guidelines Establishing Information Security Standards,[131] which obliged US banks to establish information security pro-

[126] Examples of positive development are cases Zappos.com, Inc., 888 F.3d 1020 (9th Cir. 2018) and Hutton v. Nat'l Bd. of Exam'rs in Optometry, Inc., 892 F.3d 613 (4th Cir. 2018).

[127] NEUBURGER, J. Trends in Privacy and Data Security. In: *Thomson Reuters*. p. 29. [online]. 2019 [2020-10-02]. Available at: <https://store.legal.thomsonreuters.com/law-products/news-views/corporate-counsel/trends-in-privacy-and-data-security>.

[128] ABRAMS, R. Target to Pay $18.5 Million to 47 States in Security Breach Settlement. In: *The New York Times* [online]. 2017 [2020-10-02]. Available at: <https://www.nytimes.com/2017/05/23/business/target-security-breach-settlement.html>.

[129] PENNSYLVANIA OFFICE OF ATTORNEY GENERAL. AG Shapiro Secures $600 Million from Equifax in Largest Data Breach Settlement in History. In: *Press Office* [online]. 22. 7. 2019 [2020-10-02]. Available at: <https://www.attorneygeneral.gov/taking-action/press-releases/ag-shapiro-secures-600-million-from-equifax-in-largest-data-breach-settlement-in-history/>.

[130] Gramm–Leach–Bliley Act (1999), Public Law 106–102, 113 Stat. 1338.

[131] CODE OF FEDERAL REGULATIONS. *12 CFR Appendix F to Part 225 – Interagency Guidelines Establishing Information Security Standards* [online]. 2012 [2020-10-02]. Available at: <https://www.govinfo.gov/app/details/CFR-2012-title12-vol3/CFR-2012-title12-vol3-part225-appF/summary>.

grams with adequate response measures. Obligatory components include procedures for notifying the data breach to bank's primary federal regulator as soon as possible after detection of the incident concerning sensitive customer information,[132] as well as communication to the affected customers when warranted.[133] This is further specified as situation, when the bank determines an occurring or reasonably possible misuse of the customer's personal data. Postponing the notification is justifiable by a written request from an appropriate law enforcement agency to prevent interference with a pending criminal investigation.[134] The Federal Trade Commission issued standards for safeguarding customer information applicable to non-banking financial institutions in 2002;[135] however, these do not specifically oblige the entities to notification of the data breach, but merely to timely and effective detection and response measures.

As for the medical sector, the data breach notification gained federal level anchor through the 2009 amendment of the Health Insurance Portability and Accountability Act (HIPAA)[136] through the Health Information Technology for Economic and Clinical Health Act (HITECH), in particular its Section 13402.[137] This legal instrument was further specified through the rule of Department of Health and Human Services.[138] It encompasses unsecured protected health information.[139] The definition of data breach is further narrowed by exceptions including limited unintentional access or use by an employee of a covered entity in good faith and within the scope of authority; limited inadvertent disclosure by a person who is authorized to access to another person authorized to access at the same covered entity; or a disclosure in good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.[140] Furthermore, an incident is not perceived as a data breach, if the risk of compromise of the affected protected health information is of a low probability.[141] The affected individual is to be notified without unreasonable delay after the data breach was discovered, or would have been discovered, if reasonable diligence was exercised,[142] but no later

[132] "*For purposes of the Guidance, sensitive customer information means a customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account. Sensitive customer information also includes any combination of components of customer information that would allow someone to log onto or access the customer's account, such as user name and password or password and account number.*" See Ibid. pp. 331–332.

[133] Ibid. p. 331.

[134] Ibid.

[135] FEDERAL TRADE COMMISSION. 16 CFR Part 314 Standards for Safeguarding Customer Information; Final Rule p. 36493. In: *Govinfo* [online]. 2002 [2020-10-02]. Available at: <https://www.govinfo.gov/content/pkg/FR-2002-05-23/pdf/02-12952.pdf#page=11>.

[136] Health Insurance Portability and Accountability Act (1996), 110 STAT. 1936 Public Law 104-191.

[137] Health Information Technology for Economic and Clinical Health Act (2009), 123 STAT. 226 Public Law 111-5.

[138] U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES. 45 CFR Parts 160 and 164 Breach Notification for Unsecured Protected Health Information; Interim Final Rule p. 42767. In: *Govinfo* [online]. 24. 8. 2009 [2020-10-02]. Available at: <https://www.govinfo.gov/content/pkg/FR-2009-08-24/pdf/E9-20169.pdf>.

[139] The HSS rule provides detailed specification of the terms, which indicates rather narrow scope of the obligation. Ibid. p. 42768.

[140] Ibid. p. 427687, s. 164.402(2).

[141] Ibid.

[142] Ibid. p. 427688 s. 164.404 (a).

than in 60 days.[143] If more than 500 individuals in the given state are affected, prominent state media outlets are to be notified as well within similar timeframe.[144] Data breach affecting 500 or more individuals shall the entity further report to the Department of Health and Human Services. Basic information about such cases are then made public through the Breach Portal, allowing for transparency and better information dissemination.[145] Smaller data breaches should be documented and reported jointly at the end of the calendar year.[146] If the data breach is discovered by a business associate of the covered entity, there is a similar obligation to notify the covered entity latest within 60 days, also counting the time based on the presumption of detection following reasonable diligence.[147] This sub-obligation can be likened to the relationship between processor and controller under the European data protection regime.

The scope of medical sector specific data breach notification was further broadened by the Section 13407 of the HITECH Act.[148] It applies to vendors of personal health records and their third-party service providers not subject to the authority of HHS. This instrument was specified through parallel rule of the Federal Trade Commission.[149] The understanding of data breach for the purpose of this application differs from the HIPAA-covered entities. The scope is realigned towards unsecured electronic personal health records containing identifiable health information. It is further limited in definition to acquisition of such information without the authorization of the individual. The burden of proof regarding absence of unauthorized access lies with the vendor of personal health records, PHR related entity, or third-party service provider that experienced the breach.[150] Apart from these differences, the section and subsequent FTC rule provide for similarly structured data breach notification obligation as in case of above described HHS rule. The vendors of personal health records are obliged to communicate the data breach to the affected individuals as well as notify the Federal Trade Commission, which is further obliged to report the data breach to the HHS.[151] Third party service providers then stand in the secondary position with notification obligation towards the vendor.[152] The time limit of 60 days is present, as is the related law enforcement exception.[153] The form of notice and communication to

[143] Ibid. p. 427688 s. 164.404 (b).
[144] Ibid. p. 427688 s. 164.406.
[145] U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES. Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information. In: *U.S. Department of Health and Human Services Office for Civil Rights* [online]. 2020 [2020-10-02]. Available at: <https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf>.
[146] U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES. 45 CFR Parts 160 and 164 Breach Notification for Unsecured Protected Health Information; Interim Final Rule p. 427688 s. 164.408. In: *Govinfo* [online]. 24. 8. 2009 [2020-10-02] Available at: <https://www.govinfo.gov/content/pkg/FR-2009-08-24/pdf/E9-20169.pdf>.
[147] Ibid. p. 427689 s. 164.410.
[148] Health Information Technology for Economic and Clinical Health Act (2009), 123 STAT. 226 Public Law 111-5, p. 226.
[149] FEDERAL TRADE COMMISSION. 16 CFR Part 318 Health Breach Notification Rule; Final Rule p. 42980. In: *Govinfo* [online]. 25. 8. 2009 [2020-10-02]. Available at: <https://www.govinfo.gov/content/pkg/FR-2009-08-25/pdf/E9-20142.pdf>.
[150] Ibid. p. 42980 s. 318.2 (a).
[151] Ibid. p. 42980 s. 318.3 (a).
[152] Ibid. p. 42980 s. 318.3 (b).
[153] Ibid. p. 42981 s. 318.4.

media in case of data breach affecting over 500 individuals are similar to HHS rule. The notice to FTC in case of such larger breach shall take no more than 10 business days.[154]

4.5 FTC activity concerning data breach notification

As evident from its partial authority over entities processing financial and medical personal data, the regulatory role of the FTC with regard to data breach notification is considerable. Apart from already mentioned direct competence links, another can be found through the jurisdiction over "unfair or deceptive acts or practices".[155] This basis of authority for investigation into data breach notification practices is, however, continuously challenged, as it is inferred indirectly from misleading privacy policies or failure to implement and act upon such policy pursuant to FTC rules or standards.[156] Nevertheless, there is frequent activity of the FTC on this basis concerning consequences of data breaches, for example in the matters of Wyndham Hotels and Resorts data breach in 2015,[157] AshleyMadison.com data breach in the same year[158] or 2016 LightYear Dealer Technologies data breach.[159]

In consequence, the activity of FTC complements the coordinated actions of the Attorney Generals and creates the basis for enforcement of compensation for the affected individuals under the US data breach legal framework, despite conceptual inclination of the statutes towards private actions rather than protection through the public authorities.

4.6 Federal law

The urgency of the need for harmonized approach to data breach reporting within the United States is recognized and discussed in expert as well as administrative and political circles ever since major disrupting data breaches became frequent occurrence.[160] A par-

---

[154] Ibid. p. 42981 s. 318.5.

[155] Wheeler-Lea Amendments of the Federal Trade Commission Act (1938), Public Law 75-447, 52 Stat. 1 to the 15 U.S.C. § 45 Section 5.

[156] UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE. INFORMATION RESELLERS: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace p. 11. In: *U.S. Government Accountability Office* [online]. 2013 [2020-10-02]. Available at: <https://www.gao.gov/assets/660/658151.pdf>; MURRAY, T. 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, Vol. 94, No. 1, p. 140.

[157] OFFICE OF PUBLIC AFFAIRS. Wyndham Settles FTC Charges It Unfairly Placed Consumers' Payment Card Information At Risk. In: *Federal Trade Commission* [online]. 9. 12. 2015 [2020-10-02]. Available at: <https://www.ftc.gov/news-events/press-releases/2015/12/wyndham-settles-ftc-charges-it-unfairly-placed-consumers-payment>.

[158] OFFICE OF PUBLIC AFFAIRS. Operators of AshleyMadison.com Settle FTC, State Charges Resulting From 2015 Data Breach that Exposed 36 Million Users' Profile Information. In: *Federal Trade Commission* [online]. 14. 12. 2016 [2020-10-02]. Available at: <https://www.ftc.gov/news-events/press-releases/2016/12/operators-ashley-madisoncom-settle-ftc-state-charges-resulting>.

[159] OFFICE OF PUBLIC AFFAIRS. FTC Gives Final Approval to Settlement with Auto Dealer Software Company That Allegedly Failed to Protect Consumers' Data. In: *Federal Trade Commission* [online]. 6. 9. 2019 [2020-10-02]. Available at: <https://www.ftc.gov/news-events/press-releases/2019/09/ftc-gives-final-approval-settlement-auto-dealer-software-company>.

[160] JOERLING, J. Data Breach Notification Laws: An Argument for a Comprehensive Federal Law to Protect Consumer Data. *Washington University Journal of Law & Policy*. 2010, Vol. 32, pp. 468–470.

ticularly strong message was sent by the major data breach of 2013 by the retail giant Target. In reaction, many influential voices were raised in support of harmonized data breach notification legislation. Among them that of the U.S General Attorney Eric Holder[161] or Edith Ramirez, Chairwoman of the Federal Trade Commission, who stressed that: "[n]*ever has the need for* [federal data security and breach notification] *legislation been greater.*"[162] Support for such legislation was expressed also by the industry associations.[163] There was no shortage of attempts to respond to this issue and multiple bills were proposed over the following period in order to remedy the lack of harmonized approach to data breach notification in the United States. The year 2014 saw the introduction of a number of bills including the Cybersecurity Information Sharing Act of 2014,[164] Personal Data Privacy and Security Act of 2014,[165] Data Security Act of 2014,[166] Data Security and Breach Notification Act of 2014[167] as well as Personal Data Protection and Breach Accountability Act of 2014.[168] Further attempt came from the Obama administration, who was strong proponent of the previous attempts[169] and introduced a bill for Personal Data Notification and Protection Act[170] in 2015. All these proposals incorporated provisions on harmonized data breach notification obligation, however, none of these were passed into law.[171]

Another wave of proposals[172] came in reaction to the major data breach of Equifax in 2017.[173] These included the bills on Secure and Protect Americans' Data Act of 2017,[174]

[161] Industry Backs Attorney General's Call for Federal Data-Breach Law. In: *AdAge* [online]. 25. 2. 2014 [2020-10-02]. Available at: <https://adage.com/article/privacy-and-regulation/industry-backs-ag-s-call-federal-data-breach-law/291865>.

[162] RAMIREZ, E. *Prepared Statement of the Federal Trade Commission On Privacy In the Digital Age: Preventing Data Breaches and Combating Cybercrime* Washington DC: United States Senate. [online]. 3. 2. 2014 [2020-10-02]. Available at: <https://www.ftc.gov/public-statements/2014/02/prepared-statement-federal-trade-commission-privacy-digital-age-preventing>.

[163] SASSO, B. Business groups call for data breach law. In: *The Hill* [online]. 18. 7. 2013 [2020-10-02]. Available at: <https://thehill.com/policy/technology/312163-overnight-tech-business-groups-call-for-data-breach-law>.

[164] Bill for Cybersecurity Information Sharing Act, S. 2588, 113th Cong. (2014).

[165] Bill for Personal Data Privacy and Security Act, S. 1897, 113th Cong. (2014).

[166] Bill for Data Security Act, S. 1927, 113th Cong. (2014).

[167] Bill for Data Security and Breach Notification Act, S. 1976, 113th Cong. (2014).

[168] Bill for Personal Data Protection and Breach Accountability Act, S. 1995, 113th Cong. (2014).

[169] GROSS, G. Obama calls for data breach notification law, privacy bill of rights. In: *PCWorld* [online]. 2015 [2020-10-02]. Available at: <https://www.pcworld.com/article/2867872/obama-calls-for-data-breach-notification-law-privacy-bill-of-rights.html>.

[170] Bill for Personal Data Notification and Protection Act, H.R. 1704, 114th Cong. (2015-2016); SHEAR, M., SINGER, N. Obama to Call for Laws Covering Data Hacking and Student Privacy. In: *The New York Times* [online]. 2017 [2020-10-02]. Available at: <https://www.nytimes.com/2015/01/12/us/politics/obama-to-call-for-laws-covering-data-hacking-and-student-privacy.html>.

[171] NEWMAN, B. Hacking the Current System: Congress' Attempt to Pass Data Security and Breach Notification Legislation. *Journal of Law, Technology and Policy*. 2015, Vol. 2015, pp. 438 et seq.

[172] BAUTISTA, G., MERKEL, J., MOH, A. (Another) Federal Data Breach Notification Law Introduced in Congress. *The National Law Review* [online]. 18. 12. 2017 [2020-10-02]. Available at: <https://www.natlawreview.com/article/another-federal-data-breach-notification-law-introduced-congress>.

[173] KREBS, B. Equifax breach. In: *Krebs on Security* [online]. 10. 10. 2017 [2020-10-02]. Available at: <https://krebsonsecurity.com/tag/equifax-breach/page/2/>.

[174] Bill for Secure and Protect Americans' Data Act, H.R.3896, 115th Cong. (2017–2018).

Cyber Breach Notification Act of 2017,[175] Data Security and Breach Notification Act of 2017,[176] Personal Data Notification and Protection Act of 2017,[177] Identity Theft and Tax Fraud Prevention Act of 2017,[178] Online Privacy Act of 2017[179] as well as the bill to require notification following a breach of security of a system containing personal information, and for other purposes of 2017.[180] Neither any of this set of proposed bills resulted in a law as of yet.

So far, the latest wave of discussion on federal data breach notification legislation[181] erupted in spring of 2018, following the Facebook Cambridge Analytica scandal,[182] further enhanced through the coming in force of the General Data Protection Regulation 2016/679 in the European Union, which affected many US entities as controllers of European personal data and let to large scale mobilisation of user awareness about personal data protection and privacy.[183] As shown in recent interactions between the consumer advocates and representatives of the industry, the joined support for a federal level legislation of data breach notification hinders on the contradictory visions of its contents, as the interests of these camps largely collide. Whereas the former group promotes robust privacy measures shifting burden and costs from consumers to companies,[184] the latter targets softer federal law unifying the regulatory requirements and limiting state level tendencies towards stricter requirements.[185]

Following from this brief overview of legislative developments on the federal level, the absence of unified approach to data breach notification within the US law can be seen as vivid reminder of the broadly present deep rift between the camp pursuing enhanced privacy and larger control of the users over their virtual presence and the representatives of the industry build on the principles of surveillance capitalism.[186]

---

[175] Bill for Cyber Breach Notification Act of 2017, H.R.3975, 115th Cong. (2017–2018).
[176] Bill for Data Security and Breach Notification Act, S.2179, 115th Cong. (2017–2018).
[177] Bill for Personal Data Notification and Protection Act, H.R.3806, 115th Cong. (2017–2018).
[178] Bill for Identity Theft and Tax Fraud Prevention Act, S.606, 115th Cong. (2017–2018).
[179] Bill for Online Privacy Act, H.R.3175, 115th Cong. (2017–2018).
[180] Bill to require notification following a breach of security of a system containing personal information, and for other purposes, H.R.3816, 115th Cong. (2017–2018).
[181] LAPOWSKY, I. Get Ready for a Privacy Law Showdown in 2019. In: *Wired* [online]. 2018 [2020-10-02]. Available at: <https://www.wired.com/story/privacy-law-showdown-congress-2019/>.
[182] SCHNEIER, B. Facebook and Cambridge Analytica. In: *Schneier on Security* [online]. 29. 3. 2018 [2020-10-02]. Available at: <https://www.schneier.com/blog/archives/2018/03/facebook_and_ca.html>.
[183] As GDPR nears, Google searches for privacy are at a 12-year high. In: *The Economist* [online]. 2018 [2020-10-02]. Available at: <https://www.economist.com/graphic-detail/2018/05/21/as-gdpr-nears-google-searches-for-privacy-are-at-a-12-year-high>.
[184] BLOOMBERG, S. Tech Industry & Consumer Advocates Share Support for Federal Data-Privacy Legislation, Differ on the Details. In: *Security, Privacy and the Law* [online]. 18. 10. 2018 [2020-10-02]. Available at: <https://www.securityprivacyandthelaw.com/2018/10/tech-industry-consumer-advocates-share-support-for-federal-data-privacy-legislation-differ-on-the-details/>.
[185] SCHNEIER, B. California Passes New Privacy Law. In: *Schneier on Security* [online]. 3. 7. 2018 [2020-10-02]. Available at: <https://www.schneier.com/blog/archives/2018/07/california_pass.html>.
[186] ZUBOFF, S. Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*. 2015, Vol. 30, No. 1, pp. 75 et seq.

5 SUMMARY OF PART I AND CONTENT OF THE PART II

This part of the contribution introduced the reader to the concept of personal data breach and its relevance in nowadays digital society. We described the context, in which data breaches occur, in particular as cyber security incidents, and the harm that they cause to individuals as well as affected businesses. Subsequently we compared the EU and US perspective and set the legal definition of personal data breach applicable to this contribution. The main focus of this part was the relevant legal framework of the United States, however, first some relevant specifics of the US law had to be highlighted. The US data breach notification legislation was presented in detail, firstly through the California statute and then through overview of statutes in other US states and the sector-specific federal laws. The discussion touched upon the issue of available case law, current tendencies towards settlement and role of the Attorney Generals and FTC. Additionally, the attempts for unified federal law were also described.

The Part II of this contribution shall add the insight into the respective EU regulatory approach and contains the discussion of the parallels of the US and EU frameworks and available insight to be drawn from this doctrinal research.