TALLINN UNIVERSITY OF TECHNOLOGY

Faculty of Social Sciences
Tallinn Law School

Jesse-Richard Honkasalo

Big Data and the U.S. Private Sector - Imbalance between the Rights of Data Subjects and the Rights of Data Controllers?

Bachelor Thesis

Supervisor: Kari Käsper, MA

Tallinn 2017

List of Acronyms

ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
BD	Big Data
CRA	Consumer Reporting Agency
COPPA	Children's Online Privacy Protection Act
DOT	Department of Transportation
FAA	Federal Aviation Agency
FTC	Federal Trade Commission
FCC	Federal Communications Commission
FTCA	Federal Trade Commission Act
FCRA	Fair Credit Reporting Act
GLB	Gramm-Leach-Bliley-Act
HIPAA	Health Insurance Portability and Accountability Act
ICT	Information and Communication Technology
ISP	Internet Service Provider
NCSA	National Cyber Security Alliance
PII	Personally Identifiable Information
SSA	Social Security Administration
SCOTUS	The Supreme Court of the United States
URL	Uniform Resource Identifier
VRPA	Video Rental Privacy Act
VPPA	Video Privacy Protection Act

Table of Contents

1. Introduction

1.1 Background and Aim of the Research

Personal and non-personal data have become a commodity in the U.S. over the last decade and this fast development has been noted amongst many scholars by referring to the so called revolutionary era of Big Data (BD) or "datafication". In 2013 McKinsey Global Institute approximated that Big Data will yield 610 billion USD annually in overall productivity and cost savings.[1] Considering the aforesaid monetary incentive it is not a surprise that many capable private sector actors have started to employ Big Data as a central part of their daily business activities. This has raised many questions whether the utilitarian nature of Big Data will outweigh problems stemming from data privacy and individual autonomy.[2] Another reason for the strong appeal to Big Data has been the gradual decrease in costs regarding collection and storage of data due to rapid technological advancement[3] in the field of data science and ICT (information and communication technology). Figuratively, on the opposite side of the table facing Big Data supporters as a counterpoise are privacy advocates who have tried to step-wisely increase consumer awareness about concerns of data privacy. In 2016 TrustE in collaboration with National Cyber Security Alliance (NCSA) published the U.S. Consumer Privacy Index of 2016. According to it 31% of Americans understand how companies share their personal information, 92% are afraid of their privacy online, and the primary cause of concern are companies that share personal information with other companies.[4]

The current data privacy regime in the U.S. has received a lot of critique from its counterpart regime in EU for not having an omnibus data protection law, and this in turn has greatly impeded Americans' efforts to substantiate effectiveness of the U.S.'s sectoral approach to data privacy protection.[5] In addition, the complex nature of the U.S. data privacy protection tends to usher academics who are interested in privacy matters to give scathing reviews of the protection afforded

[1] Kshetri, N. Big data's impact on privacy, security and consumer welfare, *Telecommunications Policy (2014)*, p.1
[2] Clinton D. Lanier, Jr., Amit Saini, Understanding Consumer Privacy: A Review and Future Directions, Academy of Marketing Science Review volume 12, 1.1.2008, p.17
[3] Max N. Helveston, Consumer Protection in the Age of Big Data, *Washington University Law Review, Vol. 93, 2016*, p.25
[4] 2016 TRUSTe/NCSA Consumer Privacy Infographic – US Edition, <www.truste.com/resources/privacy-research/ncsa-consumer-privacy-index-us/>(05.01.2017)
[5] Alan Charles Raul, The Privacy, Data Protection and Cybersecurity Law Review - Edition 1, November 2014, p.6

by the above-mentioned sectoral approach.[6] Recent debate revolving around Big Data, however, is deeply focused on contemplating the possibilities it might bring about in varying industries (e.g. insurance industry) or negative effects it might have on natural persons (e.g. consumers) in the future. Also BD analytics in relation to State's security interests and commercial advertising techniques (namely consumer profiling) used by private entities has gained considerable attention amidst scholars. Relatively little attention is given to an important question; how the U.S. core privacy statutes reflect the rights of data subjects or data controllers within the realm of Big Data today?

Therefore the aim of the research is to elucidate whether an imbalance between the rights of data subjects and the rights of data controllers (i.e. private sector business entities) that engage in BD for purely commercial purposes exists or not; or whether the current state of affairs indicates that there isn't any balance at all between the rights of data subjects and data controllers under the current U.S. data privacy regime. While the author tries to formulate a comprehensive answer to the aforementioned main question, one should note that the U.S. does not have a comprehensive data privacy legislation in place[7] and the American concept of privacy slightly differs from its European counterpart.[8]

1.2 Research Methodology

The research conducted will be primarily based on secondary research (desktop research), which comprises of multiple sources including various articles and texts addressing American data privacy protection. All of the articles and texts have been published by academics or experts in the field of data privacy. Secondly, comparative analysis will be applied in order to further determine the main question of the thesis; is there an actual imbalance between the rights of data subjects and data controllers with respect to utilization of Big Data and how the current data privacy regime reflects these rights? Attention will be paid to case law and to the current key U.S federal statutes regulating privacy matters, and examples of state level privacy protection will be derived from the state of California owing to its comprehensive codification and efforts made in the progress of further regulating protection of privacy.

---

[6] An ESET White Paper by Stephen Cobb, Data Privacy and data protection: US law and legislation, April 2016, p.1
[7] supra note 6, p.9
[8] Winston J. Maxwell, Principles-based regulation of personal data: the case of 'fair processing', International Data Privacy Law (2015) 5 (3): 205-216, 21 July 2015, p.207

1.3 Reasons for Choosing the Topic

The author has chosen to focus on a privacy related matter due to his interest towards American common law and developments taking place in the business practices of private entities. The emergence of the differing term 'Big Data' has also found its way into many academic publications that especially address varying concerns of data privacy with respect to the American sectoral approach. Along with above stated reasons, the author will focus on the U.S. data privacy due to its highly received criticism and in consequence of the axiomatic commercialization of personal data of American consumers.

Most importantly - the author recognizes an opportunity for contributing to the discussion pertaining to Big Data's effects on consumer privacy. Thus, arriving to a conclusion regarding the question indicated in **Chapter 1.1**; whether an imbalance between the rights of data subjects and the rights of data controllers (i.e. business entities) that engage in BD utilization for purely commercial purposes exists or not, and how it manifests under the current U.S. data privacy regime.

The next Chapter will start off with a short abstract of how Big Data is ultimately defined and why it should not be confused with the term data mining. Further, discussion about the prominent BD actors in the private sector will be dealt with; views of BD's potential benefits and harms shall be addressed as briefly as possible; American notion of privacy shall be covered, and after that the discussion will be directed to addressing the main question of the research in the light of U.S. core data privacy legislation and case law.

2. Big Data and U.S. Private Sector

2.1 The Many Definitions of Big Data

According to a variety of different studies a single definition accepted as standard for the term Big Data does not yet exist.[9] Despite the divergent definitions as regards the term BD, the most common denominator correlates to the overall size of different data categories produced on a daily

[9] Abu Bakar Munir, Siti Hajar Mohd Yasin, Firdaus Muhammad-Sukki, Big Data: Big Challenges to Privacy and Data Protection, World Academy of Science, Engineering and Technology International Journal of Social, Education, Economics and Management Engineering Vol:9, No:1, 2015, p.355

basis. The amount of data produced daily is calculated in quintillion bytes and more than a decade ago, in 2003, it was estimated that the amount of information stored every year globally grew by 161 exabytes - 5 exabytes is comparable to information stored in the U.S. Library of Congress.[10] Sources of BD range from normal daily transactions to social media posts,[11] in other words every imaginable way of generating data today (i.e. transactions leaving a digital footprint) could be associated as a source to accumulation of BD.

In contrast to the common connection made between the amount of data generated and collected in reference to BD, it has been stated that more focus should paid to 'the capacity to search, aggregate, and cross-reference large data sets' in order to conclusively to define what constitutes the core elements of BD.[12] Pursuant to the above-said notion, an enormous single database filled only with certain type of information should not be considered as BD per se, however, if the information contained in a database is complemented by other disparate datasets and specific type of method/technology is required for the completion of a data analysis; such type of combination could be characterized as Big Data analytics.[13]

What ties all of the different definitions of BD together is still nonetheless heavily linked to the sheer magnitude of varying information underlying the perception of BD. Typically three pertinent features are ascribed to its definition; high-volume (dataset size is not comparable to a typical database and its analysis/storage requires special technologies); high-velocity (the overall amount of data generated is rapid - it requires fast storage and analysis); and lastly high-variety (disparate datasets formulate the overall structure of data).[14] Alongside with high-volume, high-velocity and high-variety stands notion of BD's potential. Companies like the IBM prefer to compound the essence of BD to its opportunity of revealing insights concerning new content and data created in the process of "mining" BD rather than simply referring to its vast size only.[15] All in all, despite the many different views of what actually qualifies as BD, majority of experts stand behind the three pertinent features stated above.

[10] Id.
[11] Id.
[12] supra note 3, p.10
[13] Id.
[14] supra note 10, p.356
[15] Id.

2.2 Big Data v. Data Mining

When discussion revolves around Big Data it is common to juxtapose data mining with the former. This is not completely right nor entirely wrong because to some extent BD can be understood as a really powerful form of data mining.[16] The main purpose behind utilization of BD is to indeed reveal hidden patterns or correlations between disparate sets of data.[17] Nevertheless, BD should be understood as a large vessel of divergent information, which is driven by versatile data mining techniques. Instead of using both terms in an interchangeable manner, data mining should be only regarded as an essential part in the course of carrying out BD analytics.

According to Daniel J. Solove & Chris Jay Hoofnagle: "data mining involves searching through repositories of data to find out new information by combining existing pieces of data or to make predictions about future behavior based on patterns in the data."[18] If the purpose of data mining is confused with the almost analogous objective of BD analytics, it would render most data handling methods being categorized as BD technologies. For the reason being it should be remarked that data mining and BD analytics should not be considered in equal terms.

2.3 Categorization of BD Actors

The so called "players" belonging in the sphere of BD can be divided into four groups, all of which represents their main functions with respect to utilization of data.[19] The first group is referred as data collectors (i.e. someone who collects data generated by data subjects with or without the latter's consent - the data generated can vary from CCTV footage to credit card readers and every piece of this information is eventually stored for a specific purpose or sold/rented to third parties); the second group is called as data markets (these platforms have been created for individuals, companies, government agencies and marketing organizations that seek specific sets of data for their own needs); the third group is titled as data users (refers to people and organizations who have access to data, whether free of charge or not, via applications e.g. retail analytics); and the

[16] Ira S. Rubinstein, Big Data: The End of Privacy or a New Beginning?, International Data Privacy Law, 2013, Vol. 3, No. 2, p.74
[17] Id.
[18] Daniel J. Solove & Chris Jay Hoofnagle, A MODEL REGIME OF PRIVACY PROTECTION Version 2.0, 05.04.2005, p.6
[19] Terence Craig, Mary E. Ludloff, Privacy and Big Data, O'Reilly Media, September 2011, p.45

last group is known as data monitors (agencies and organizations that oversee industries' data privacy practices).[20]

In order to name a few prominent American private sector companies belonging in the category of "data collectors"; Yahoo, Microsoft, Google, Facebook, Twitter and Amazon are perfect examples of businesses that to a significant degree rely on influx of high-volume, high-variety and high-velocity data. Additionally, companies specialized in selling consumer information, namely lucrative data brokers such as Acxiom and Experian can be regarded as one of the many players in the exploitation of Big Data. As the current economy has evolved into entailing data-driven business models, several companies operating in the private sector (e.g. Facebook) have shifted from passive data collection to active data collection through various user experiments.[21] This has raised disquietude and the concerns have been further exacerbated by federal and state governments' deep interests in massive amounts of data held by the private sector companies.[22] Taking into account the importance of data mining in respect of large private sector enterprises taking part in online commerce and companies that build their business models around online advertising,[23] it is common practice to minimize individual users' control over their data under such instances. The idea of giving consumers or users significantly more control over their data and changing to a model of business that requires re-notifying consumers whenever data is used for new purposes is arguably seen as counterproductive due to its likelihood of placing burden of privacy protection on the individuals instead of the companies engaged in BD.[24] It would also be extremely cumbersome to apply consent and notice requirements as regards the immense size and divergence of datasets constituting BD altogether. On the other hand, majority of privacy advocates highly root for the traditional approach of notice and consent requirements.

One of the main reasons why the private sector plays a significantly higher position in contrast to the public sector in data retention is caused by the former being susceptible to market pressures and economic incentives created in the wake of BD's remarked potential.[25] Secondly, as it was mentioned before; federal and state governments are desperate to gain unfettered access to personal

[20] Id.
[21] Victoria D. Baranetsky, Social Media and the Internet: A Story of Privatization, 35 PaceL. Rev. 304 (2014), p.307
[22] Id., p.309
[23] supra note 17, p.86
[24] supra note 10, p.360-361
[25] Joel Reidenberg, The Data Surveillance State in Europe and the United States, 49 Wake Forest L. Rev. 583 (2014), p.602

data retained by the private sector firms. In fact, back in 2011 Google's Transparency Report established that law enforcement had made over 1.3 million requests for user data and the numbers are increasing drastically.[26] That is to say that the era of BD or datafication has rendered the private sector indirectly 'responsible for the protection of societal rights' and this development is aggravated by U.S.'s indolence of enacting a piece of legislation which would lay down general data retention requirements.[27]

Considering all the factors stated above, it is evident that capable private sector players are more directly involved in the employment of BD than public sector actors for the time being. Despite the many concerns raised by private sector technology companies' capabilities of collecting, analyzing and organizing large amounts of data, from a law enforcement point of view data collection is accounted as a public function or resource.[28] However, the consequences of law enforcement privatization, online commerce, commercial advertising and how various enterprises *de facto* operate within the realm of BD is beyond the scope of the research. Pointing out the private sector's data collection and its influence on the public sector with regard to law enforcement was necessary in order to further illustrate the intrinsic value in personal data recognized today. To the same extent it is essential to conceive that BD analytics requires particular resources and the most prominent private sector players are more likely capable of utilizing BD than newcomers or publicly funded organizations and agencies. Exceptions within the public sector, such as intelligence agencies, should be disregarded in terms of direct BD participation because of their involvement in law enforcement matters and state agency status. Consequently, the increased reliance on access to personal data held by the private sector firms indicates a fundamental change in the practice of protecting societal rights.[29]

2.4 Big Data and Privacy Related Concerns

Many of the privacy concerns raised during the emergence of BD are to a great extent notification, control, access and security related problems.[30] Consumers want to be aware of how their information is collected and used by firms; in a relative manner consumers want to know that their own decisions have the potential to affect how their personal information will be shared amongst

[26] Id., p.595
[27] Id., p.585, 601
[28] supra note 22, p.341
[29] supra note 26, p.601-602
[30] supra note 2, p.4

companies (e.g. an individual does not want to share their personal data to other firms); and lastly consumers want to be certain that in exchange of providing personal data firms clearly set up adequate data protection measures for the protection of personal data provided.[31] Nevertheless, as stated in **Chapter 2.3**, re-notifying consumers whenever data is used for new purposes is regarded counterproductive due to its likelihood of placing burden of privacy protection on the individuals instead of the companies engaged in the handling of personal data. What further makes the task of informing consumers at a relevant moment more difficult is the lack of transparency as regards processing of personal data.[32] It has been noted that private sector firms (e.g. data brokers, ad networks and analytics firms) operate behind the curtains with data provided by the consumers and this current practice erodes the necessary transparency required to provide consumers with better understanding of BD analytics and how such data practices can affect data subjects altogether.[33]

Another concern emanates from the fairness of BD analytics, and focus on this point is often directed towards data brokers who specialize in profiling and analyzing consumer particular information. When data brokers compile consumer profiles, they also cast them into segments or specific categories that may contain character specific titles such as 'financially challenged' or 'diabetes interest'.[34] If these aforesaid profiles are used in automated decision making, especially in the insurance industry, or banking where loans are granted on the basis of individuals' credit scores, it is highly likely that the probability of unlawful discrimination incidents taking place will increase.[35] Although the Equal Credit Opportunity Act prohibits using characteristics like race and gender in determination of one's creditworthiness, predictable analysis carried out via application of BD may unintentionally infer gender or race through other datasets like zip code or product preferences, both of which are inputs not proscribed by law.[36] There are other concerns as well. Apart from unintentional discrimination, special attention should be paid to data quality, which is a seemingly challenging task when the sheer magnitude of divergent datasets is taken into account in association with the very definition constituting actual BD. The process of collecting and processing data for purely analytical purposes may yield multiple errors and completely derail

[31] Id.
[32] U.S. Federal Trade Commissioner Julie Brill, Privacy and Data Security in the Age of Big Data and the Internet of Things, Delivered at Washington Governor Jay Inslee's Cyber Security and Privacy Summit January 5, 2016, p.8
[33] Id, p.7
[34] Id, p.8
[35] Id, p.9
[36] K. Krasnow Waterman, Paula J. Bruening; Big Data analytics: risks and responsibilities. *International Data Privacy Law* 2014; 4 (2): 89-95, p.94

analytical models, if sources of data or collection practices are not closely monitored.[37] One of the main problems in the current data privacy regime is the fact that it does not take into consideration the various nuances linked to the application of BD analytics, such as producing actual PII through inferences or by examining data patterns leading to prediction concerning data subjects.[38] Respectively, the White House report on Big Data published on May 2016 reiterated same concerns regarding BD: "if these technologies are not implemented with care, they can also perpetuate, exacerbate, or mask harmful discrimination".[39]

2.4.1 Bills that were never enacted into law

In response to challenges posed by the gradually growing employment of BD it has been acknowledged that new pieces of legislation should be enacted in order to mitigate privacy concerns and to further consolidate the current data privacy regime. In 2014 FTC's former commissioner Julie Briel stated that the U.S. Congress should enact a law requiring data brokers to inform consumers when personally identifiable information is processed and an option for opt-out regarding sharing of such information for marketing activities should be put in place - essentially a single piece of privacy legislation comprising of notice, access, and correction rights afforded to consumers; scaling to the nature and use of the PII in question.[40] This type of bill was introduced by Senator Markey of Massachusetts [41] on March 4, 2015, but the attempt of enacting the bill into law was unfortunately unsuccessful.[42] If the Data Broker Accountability and Transparency Act of 2015 had passed, it would have closed many gaps in the current data privacy regime pertaining to consumer privacy protection. [43]

Pursuant to Sec. 4. (b) (1) of the Transparency Act:

---

[37] Id.
[38] Id.
[39] CECILIA MUÑOZ, MEGAN SMITH, DJ PATIL, Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights, Executive Office of the President May 2016, p.4
[40] Commissioner Julie Brill, "Big Data and Consumer Privacy: Identifying Challenges, Finding Solutions", Address at the Woodrow Wilson School of Public and International Affairs Princeton, University February 20, 2014, p.8
[41] Id.
[42] S. 668 — 114th Congress: Data Broker Accountability and Transparency Act of 2015." www.GovTrack.us. 2015. <https://www.govtrack.us/congress/bills/114/s668>(12.1.2017)
[43] supra note 37

Subject to paragraph (4), a covered data broker shall provide an individual a means to review any personal information or other information that specifically identifies that individual, that the covered data broker collects, assembles, or maintains on that individual.[44]

Laying down a rule that grants consumer's access to their own PII is vital in order to preserve transparency and balance between data controllers and data subjects. The Transparency Act would have limited data brokers' purview in respect of PII, as Sec. 4 paragraph 5 would have limited data brokers' right to exploit personal information under specific circumstances. According to this limitation a data broker cannot use information collected in order to verify an individual's identity for any other purposes than the sole intention of determining one's actual identity.[45] This would have been a significant improvement considering the fact there is not currently any similar limitation in place, which would narrow the scope of data handling activities carried out by data brokers to some extent. Another noteworthy improvement would have been a clear dichotomy made between PII and non-PII under Sec. 2 paragraph (4) of the proposed Act, instead of relying on various interpretations set forth by the SCOTUS (Supreme Court of the United States) on what *de jure* constitutes PII, the Act would have drawn a straightforward distinction in that regard by leaving some flexibility in the definition of non-public information. Nonetheless, one can always speculate how the Act would have affected privacy protection, if it had been enacted into law. But it is reasonable to presume that the Act would have remarkably consolidated rather than undermined the present U.S. data privacy regime.

In Senator Markey's footsteps a slightly improved version of the Data Broker Accountability and Transparency Act of 2015 was introduced on February 10, 2016 by Henry C. "Hank" Johnson, Jr. and the Act was subsequently referred to the Committee on Energy and Commerce.[46] The main outline of the earlier Transparency Act is equivalent to the proposed Act of 2016 with few improved additions. For example, Sec. 3 paragraph (5) (a) lays down a more comprehensive definition of personal information. According to it:

The term personal information means an individual's first name or initial and last name, or address, or phone number, in combination with any one or more of the following data elements

[44] supra note 39, See S. 668 - Sec. 4. (b) (1)
[45] Id.
[46] H.R. 4516 — 114th Congress: Data Broker Accountability and Transparency Act of 2016." www.GovTrack.us. 2016. February 3, 2017 <https://www.govtrack.us/congress/bills/114/hr4516>(12.1.2017)

for that individual: (i) Social Security number; (ii) Driver's license number, passport number, military identification number, or other similar number issued on a government document used to verify identity; (iii) Financial account number, or credit or debit card number, and any required security code, access code, or password that is necessary to permit access to an individual's financial account.[47]

Most importantly Sec. 3 paragraph (5) (b) states that the Commission has a right to alter the definition of personal information under Section 553 of Title 5 (USC), if such action is required in response to technological advances.[48] This clause is significant due to it rendering paragraph (5) (a) highly adaptable and responsive vis-à-vis rapid technological development. Considering the high probability of new categories of personal information coming into existence, and the constant flux in data analytics and ICT, paragraph (5) (b) therefore inevitably extends protection and transparency guaranteed under the Data Broker Accountability and Transparency Act of 2016. Furthermore, if paragraph (5) (b) is applied at the right time, there is no need to include every possible category of information under paragraph (5) (a), only the most relevant and apropos categories of PII affecting individuals will be included. This in turn has a positive effect on private sector firms labelled as data brokers as well. When the line between non-personal and personal information is drawn so clearly that one cannot confuse former with the latter, a new level of transparency is achieved that benefits both parties; i.e. data controllers and data subjects. Based on such clear distinction between PII and non-PII, data brokers can draw up more effective privacy policies and security measures, which increases consumer trust and overall data security provided to individuals. But it should be noted that the Act only deals with data brokers and many prominent players in BD will not necessarily qualify as such under Sec. 3 paragraph 3; if the PII maintained, collected, assembled and subsequently sold by the commercial entity consists of its own customer or employee data.[49] For example, companies like Facebook and Google sell user data to third parties.[50] In the aforesaid circumstances it is logical to presume that Facebook or Google and companies alike will not be regarded as data brokers under Sec. 3 paragraph 3 per se, even though engaging in data brokering activities with user data generated by their customers. This "gap" in the proposed Act ascribes to sector specific nature of legislating matters belonging in the private

[47] Id., See H.R.4516 - Sec. 3 (5) (a)
[48] Id., See H.R.4516 - Sec. 3 (5) (b)
[49] Id., See H.R.4516 - Sec. 3 (3)
[50] Andrew Griffin, "Apple boss Tim Cook slams Google and Facebook for selling users' data", The Independent, Wednesday 3 June 2015. <http://www.independent.co.uk/life-style/gadgets-and-tech/news/apple-boss-tim-cook-slams-google-and-facebook-for-selling-their-users-data-10295158.html>(13.1.2017)

sector. Despite of all potential privacy protection benefits and inferential improvements derived from the Act, the proposed bill was never enacted into law.

The current trajectory of introducing new pieces of legislation addressing privacy issues in relation to BD exploitation and handling of PII has been futile on federal level. Another important bill proposed, namely H.R. 2977 (114th): Consumer Privacy Protection Act of 2015 suffered the same fate as the previous data broker transparency Acts.[51] This bill in question would have required commercial entities to notify any residents whose PII has been accessed or acquired.[52] Consumers want to know how, why and what type of personal information is collected about them,[53] Sec. 211 of the proposed Consumer Privacy Protection Act would have provided much needed transparency in connection with this issue. Despite of all unsuccessful attempts made in the process of trying to further consolidate current U.S. data privacy regime, there are still federal laws, state laws and watchdogs protecting individuals from privacy violations.

2.4.2 FCC and ISPs - broadband privacy rules facing a possible inimical change

On 23.3.17 the U.S Senate voted to remove privacy rules set by the Obama administration and enforced by the Federal Communication Commission that require internet service providers to get consent from data subjects before selling their browser history to third parties.[54] If the House of Representatives or President Trump does not oppose the proposed change, ISPs can freely sell any data contained in browser history for profit without consumers' consent or knowledge.[55] This web browser data has potential to reveal sensitive information to ISPs, for example certain internet habits might produce PII which indicates one's political views or sexual orientation.[56] Republicans have stated that the FTC should regulate the activities carried out by ISPs instead of the FCC.[57] However, the FTC's charter limits the agency's powers in relation to common carriers (i.e. home and mobile ISPs).[58] The final outcome of the proposed change is not clear, but if it takes place it

[51] "H.R. 2977 — 114th Congress: Consumer Privacy Protection Act of 2015." www.GovTrack.us. 2015. February 3, 2017 <https://www.govtrack.us/congress/bills/114/hr2977>(13.1.2017)
[52] Id., See H.R. 2977 - Sec. 211. Notice To Individuals
[53] supra note 31
[54] Jon Brodkin, "How ISPs can sell your Web history-and how to stop them", Ars Technica, 24.3.2017.<https://arstechnica.com/information-technology/2017/03/how-isps-can-sell-your-web-history-and-how-to-stop-them/>(29.3.2017)
[55] Id.
[56] Id.
[57] Id.
[58] Id.

is reasonable to presume that data subjects' rights in relation to browser data will be significantly undermined. It is also reasonable to presume that in terms of BD utilization the proposed change will further increase collection and mining of divergent consumer data.

Before the attention is directed on the current U.S. data privacy regime and scrutinization of how the current core U.S. data privacy legislation and case law reflects rights of data subjects and data controllers within the realm of Big Data, **Chapter 3.** will briefly address the definition of privacy. It was stated in **Chapter 1.1** that the American concept of privacy slightly differs from its European counterpart. Hence it will be worthwhile to remark which factors underlie the definition of American privacy according to scholars, and which definitions of privacy have been widely accepted. Attention will be paid to William Prosser's taxonomy of four privacy torts and to Daniel J. Solove's four groups of harmful activities and its subgroups.

3. Concept of Privacy (U.S.)

3.1 Implicit Right to Privacy and Various Definitions

In Europe privacy is regarded as a fundamental human right,[59] however, in the U.S. the definition of privacy is derived implicitly. In fact, the word privacy has been left out of the Constitution, the Declaration of Independence and the Bill of Rights.[60] Regardless of the fact that the U.S. Constitution does not explicitly cover the right to privacy, SCOTUS has interpreted the Bill of Rights and many of its amendments in a way which clearly affords divergent protection of privacy in respect of individuals.[61] The following are prime examples of implicit privacy protection guaranteed under the Bill of Rights against particular government actions;

"individual's right to be free from unreasonable searches and seizures by the government; the right to make decisions about issues involving 'fundamental' individual liberty interests such as contraception, abortion, marriage, procreation, child rearing, and sexual intimacy; the right not to disclose certain information to the government; the right to associate free from government

[59] Joanna Kulesza, International law challenges to location privacy protection, International Data Privacy Law, 2013, Vol. 3, No. 3, p.163
[60] Frederick S. Lane, American Privacy: The 400-Year History of Our Most Contested Right, Beacon Press (November 1, 2009), p.15
[61] Fred H. Cate and Beth E. Cate, The Supreme Court and information privacy, International Data Privacy Law, 2012, Vol. 2, No. 4, p.256

intrusion; and the right to enjoy one's own home free from intrusion by the government, sexually explicit mail or radio broadcasts, or others who would disrupt one's solitude."[62]

For decades American legal scholars have gone to great lengths in search of the most eligible definition of privacy. All of it started from an article published by two lawyers Warren and Brandeis (1890) who argued that privacy should be conceived as the right to be let alone.[63] In 1960 William Prosser coined the theory of four legal torts in respect of privacy violations and claimed privacy being a multidimensional concept.[64] According to the taxonomy of four privacy torts an individual who has suffered an actual injury can bring a lawsuit against the defendant if: (I) plaintiff's solitude, seclusion or private affairs are violated by an intrusion; (II) private facts of embarrassing nature about the plaintiff are disclosed publicly; (III) publicity that results in false portrayal of the plaintiff in the public eye; and (IV) the defendant appropriates the name and likeness of the plaintiff (i.e. identity theft).[65] This model was embraced by the contemporary U.S. courts and is still used today in many jurisdictions.[66] The classification of four privacy torts has been criticized being incomplete and lacking in substance. Case *Shibley v. Time, Inc* (*1974*) [67] made it clear that the third privacy tort does not apply to cases wherein *de facto* consumer information is forwarded from one company to another in a discreet manner (i.e. the information transferred is not made public); and case *Dwyer v. American Express Company* (*1995*)[68] denoted that the first privacy tort does not apply to circumstances wherein the plaintiff willingly provides information to a company and where the data is subsequently transferred to a third party for purposes not known by the plaintiff at the time of initial consent.[69]

Albeit the above two cases are not landmark decisions of the SCOTUS, case *Time, Inc. v. Hill* (1967)[70] set a well-known precedent concerning the third privacy tort in relation to press. The case involved a dispute arising from an article published by Time Magazine. The article in question was based on a play that loosely depicted the plaintiff family's ordeals experienced whilst held

[62] Id.
[63] supra note 2, p.7
[64] Id., p.7-8
[65] Ohm, Paul, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization (August 13, 2009). UCLA Law Review, Vol. 57, p. 1701, 2010; U of Colorado Law Legal Studies Research Paper No. 9-12. p.1733
[66] Id.
[67] Common Pleas Court of Cuyahoga County, No. 915,246., *SHIBLEY v. TIME, INC., ET AL. (1974)*
[68] Appellate Court of Illinois, First District, First Division, No. 1-92-3944., Dwyer v. American Express Co. (1995)
[69] supra note 2, p.8
[70] U.S Supreme Court, 385 U.S. 374,Time, Inc. v. Hill. (1967)

hostage by three fugitives. The plaintiff sued the Time Magazine for violation of privacy that casted the plaintiff and his family into false light in the public eye. Regardless of the untrue facts published, the SCOTUS did not hold the defendant guilty of violating plaintiff's privacy due to lack of evidence substantiating defendant's malicious intent. It was held that free debate revolving around matters of public interests is more than often based on erroneous facts and a balance must be maintained between right to privacy and freedom of press and freedom of speech - press cannot be held liable when the information published without malice is unexpectedly not true (i.e. 'press must have breathing space in case of inevitable errors').[71] This case further elucidates the narrow basis for privacy violations provided pursuant to Prosser's taxonomy of four privacy torts.

Scholars who support a unitary concept of privacy hold in high regard personal autonomy and accessibility - concept of privacy resting on individual control over data provides wider privacy protection in contrast to the multidimensional concept of privacy.[72] At the time when Prosser came up with the four categories of privacy torts, BD technologies nor the internet existed. Thus, the taxonomy of four privacy torts offers very little protection vis-à-vis PII and should be considered as a relic from the past incompatible with present-day activities involving dissemination, storage or collection of personal data. Daniel J. Solove in his paper "A Taxonomy of Privacy" (2006) states privacy being an umbrella term, which refers to a multitude of divergent and closely related 'things'.[73] The so called 'four groups of harmful activities' (information collection, information processing, dissemination of information and lastly invasion) is expanded by Daniel J. Solove in order to widen the scope of a multidimensional theory of privacy and shifting discussion from the meaning of privacy to privacy related problems.[74] The four groups of harmful activities is divided into sixteen subgroups (surveillance, interrogation, aggregation, identification, insecurity, secondary use, exclusion, breach of confidentiality, disclosure, exposure, increased accessibility, blackmail, appropriation, distortion, intrusion and decisional interference) each of which represents a specific and potential privacy harm.[75] The sole of aim of the taxonomy created by Solove is to illustrate Prosser's theory of four privacy torts as obsolete as possible.[76]

[71] Lyrissa Barnett Lidsky, R. George Wright, Freedom of the Press: A Reference Guide to the United States Constitution, Greenwood Publishing Group, 2004, p.99
[72] Id.
[73] Solove, Daniel J., A Taxonomy of Privacy. University of Pennsylvania Law Review, Vol. 154, No. 3, p. 477, January 2006; GWU Law School Public Law Research Paper No. 129., p.485
[74] Linda Koontz, CIPP/US, CIPP/G, Information Privacy in the Evolving Healthcare Environment, Health Management and Information Systems Soc, 2013, p.12
[75] Id., p.12-13
[76] supra note 64, p.478

According to Solove's taxonomy, definition of privacy can be derived from various privacy violations. Essentially any potential privacy problem falling in any of the sixteen subgroups (or main groups) contributes to the conception of privacy. For example, a hypothetical situation involving Big Data analytics reveals that persons who have made search queries about cancer treatment are more likely cancer patients than individuals who have not made such query ever in their lifetime. If this data is then accidentally leaked with personal identifiers attached, one can with relative ease unearth the real identity of John Doe query number 4923495. Under this hypothetical example the elements defining privacy emanate from the possible or actual harm caused to John Doe-4923495. That is to say that in the above-mentioned situation privacy could mean not to disclose confidential health information, represent false facts to public (if John Doe-4923495 does not have cancer), unwarranted secondary use clashing with privacy (e.g. pharmaceutical companies start to advertise cancer drugs directly to John Doe) et cetera. *Summa summarum*, Solove's taxonomy serves the definition of privacy in a more comprehensive manner than Prosser's four rather limited privacy torts, as the former manages to offer a much wider base for privacy violations. Still, Solove's and Prosser's definitions of privacy are amongst a multitude of various definitions devised over the years, but a single factor rationally connects all of the sprawling theories; violating one's privacy has the potential to cause actual harm. Even if dissimilar data privacy regimes fear different actors (e.g. private sector and state) or employ slightly different definitions of privacy, the common denominator between such regimes is the concern for chilling effects (i.e. loss of personal autonomy or individual freedoms) ensuing from an invasion of privacy.[77]

3.2 Consumer Privacy?

Definition of consumer privacy figuratively follows the same path as the definition of privacy in terms of availability of divergent theories. For example, Goodwin (1991) conceived consumer privacy as the consumer's control over information provided to companies and control over various elements constituting a market transaction.[78] Eventually the definition of consumer privacy included a notion of consumer knowledge and some ethical aspects of privacy were also attached

[77] Perri, Pierluigi and Thaw, David, Ancient Worries and Modern Fears: Different Roots and Common Effects of U.S. and EU Privacy Regulation (April 19, 2015). U. of Pittsburgh Legal Studies Research Paper No. 2016-06., p.1-2

[78] supra note 2, p.18

to it (e.g. utilitarianism, justice, relativism et cetera).[79] However, consumer privacy is not regarded as an absolute right due to common disagreements arising between consumers and firms as regards the ownership of rights to information provided by a consumer and due to individual, social and cultural factors affecting individual's perception of consumer privacy.[80] For the purpose of the research, hereinafter, consumer privacy shall be regarded as data subject's notice, access, control and correction rights.

4. Complex U.S. Data Privacy Regime from a Simplified Point of View

4.1 Constitution and 4th Amendment - Inconsistent Expectation of Privacy

The word privacy has been left out of the Constitution, the Declaration of Independence and the Bill of Rights.[81] But right to privacy is still covered by some of the amendments in an implicit manner. Especially, in the fourth amendment, particular state actions are strictly prohibited in the name of privacy. The fourth amendment prohibits unreasonable search and seizures carried out by law enforcement agencies, and the term reasonable expectation of privacy was set forth in *Katz v United States* (1967)[82] by SCOTUS's response to an incident involving wiretapping and subsequent extension of protective zone of privacy afforded under the fourth amendment.[83] The case primarily focused on a question of whether a phone booth located in public and wiretapped could be protected under the 4th amendment or not.[84] The SCOTUS ruled that despite the fact the phone booth in question was located in a public area, and as the 4th amendment protects persons instead of places, Mr. Katz's expectation of privacy was still attached to the phone booth and therefore warrantless wiretapping taking place in a public area shall be regarded against the rights provided under the 4th amendment.[85] The SCOTUS has stated that there is no reasonable expectation of privacy in relation to 'voice or writing samples, phone numbers, conversations recorded by concealed microphones, and automobile passenger compartments, trunks, and glove

[79] Id., p.19,20
[80] Id.
[81] See footnote 52
[82] U.S. Supreme Court, 389 U.S. 347, *Katz v United States* (1967)
[83] supra note 53, p.261
[84] Id.
[85] Id.

boxes'.[86] Most importantly, the 4th amendment applies only to collection of information and matters regarding utilization of collected information is beyond the scope of the 4th amendment.[87] Another noteworthy decision concerning the application of the 4th amendment is *United States v. Miller* (1976)[88]. The case deals with the determination of reasonable expectation of privacy and directs the main legal question on personal information concerning disclosure to third parties. In *United States v. Miller* the defendant was accused of running an illegal distillery and the ATF had acquired checking, savings and other financial records from the defendant's bank.[89] The defendant in response to this argued that the ATF had violated his reasonable expectation to privacy under the 4th amendment for not having an eligible basis for a search warrant.[90] Pursuant to the Bank Secrecy Act of 1970, the bank was required to maintain clientele's records for several years, however, the expectation of privacy to these records was turned down by the SCOTUS.[91] The Court reasoned that: firstly the subpoenaed bank records are not the respondent's private papers; secondly there is no legitimate expectation of privacy in checks or bank slips because such records are negotiable instruments and the information therein has been voluntarily provided by the respondent to the bank; lastly issuance of a subpoena to a third party does not violate the defendant's rights and a subpoena is sufficient enough to acquire banking records under the Bank Secrecy Act (i.e. 'greater judicial scrutiny' is not necessary).[92] This ruling has been criticized on the basis of the defendant's willingness to provide information to the bank.[93] Taking into account that the defendant merely consented to a normal business transaction between himself and the recipient of funds (i.e. the bank) whilst making a deposit, there was no actual consensus on the defendant's side that the bank could store and provide this transactional information later on to another party.[94] Nevertheless, it should be noted that the bank did not provide the transactional information to an ineligible party and acted according to rules set in the Bank Privacy Act - the information was legally passed on to the ATF in order to facilitate a criminal investigation concerning the defendant. The main concern regarding the Court's ruling stems from the notion of not having any expectation of privacy under circumstances where information is voluntarily

[86] Id., p.262
[87] Id.
[88] U.S. Supreme Court, 425 U.S. 435, *United States v Miller* (1976)
[89] Paul Rudo, "United States v. Miller: The 1976 Court Case That Determined Your Privacy Rights In The Cloud", EnterpriseFeatures, 25.08.2012.<http://www.enterprisefeatures.com/united-states-v-miller-the-1976-court-case-that-determined-your-privacy-rights-in-the-cloud/>(19.01.2017)
[90] Id.
[91] Id.
[92] supra note 80
[93] supra note 82
[94] Id.

provided to a third party. If the information in question is held by a government agent it does not make a difference under the 4th amendment and according to precedent set in *United States v. Miller*.[95]

4.1.1 *United States v. Miller* (1976) BD related ramifications

One of the most important deciding factors in the *Miller's* case was the Court's rationale concerning bank checks, influenced heavily by *California Bankers Assn. v. Shultz* (1974),[96] which made it clear that checks become property of the bank because banks cannot be regarded as neutrals in a transaction involving negotiable instruments.[97] Therefore, *Miller* had no property interests in the bank checks and his claim to expectation of privacy was turned down.[98] SCOTUS also maintained that once checks enter the banking cycle, the checks in question are as good as published information, and Mr. *Miller* accepted the risk of revealing personal information to another party when he knowingly provided all of the information contained in the checks to bank employees during an ordinary course of business.[99]

The rationale behind *United States v. Miller* raises a question in respect of BD: if personal information is currently seen as a commodity, would such information be protected by an expectation of privacy owing to property interests? Shortly, No. Even if PII is seen as a commodity, individuals do not have general property rights in personal information under the current data privacy regime and constitution. In *Feist Publications v. Rural Telephone Service Co.* (1991) the SCOTUS made clear that information contained in a database and single facts therein such as names or addresses do not qualify for copyright protection under the constitution.[100] Besides, it has been reasonably stated: "granting property rights in personal information is unlikely to achieve information privacy goals in part because a key mechanism of property law, namely the general policy favoring free alienability of such rights, would more likely defeat than achieve information privacy goals."[101] BD is high-volume (dataset size is not comparable to a typical database and its analysis or storage requires special technologies); high-velocity (the overall amount of data

[95] supra note 53, p.263
[96] U.S. Supreme Court, 416 U.S. 21, *California Bankers Assn. v. Shultz* (1974)
[97] Patrick L. Moore, United States v. Miller: Without a Right to Informational Privacy, Who Will Watch the Watchers, 10 J. Marshall J. Prac. & Proc. 629 (1977), p.636
[98] Id., p.637
[99] Id.
[100] U.S. Supreme Court, 499 U.S. 340, *Feist Publications v. Rural Telephone Service Co.* (1991)
[101] Pamela Samuelson, Privacy as Intellectual Property, 52 Stan. L. Rev.1125 (1999), p.1125

generated is rapid - it requires fast storage and analysis); and high-variety (disparate datasets formulate the overall structure of data) data sets not equivalent to data stored in a normal structured data base (**Chapter 2.3**). But the information constituting BD varies to a great degree and therefore it is possible that typical things belonging in copyright law domain (e.g. pictures, videos et cetera) may form a part in disparate data sets in respect of BD. Case *KELLY v. ARRIBA SOFT CORP*. (2003)[102] concerned a visual search engine on the Internet created by the defendant. The search engine in question acquired plaintiff's photographs and made them available to users of the defendant's search engine in a thumbnail size format while providing a link to the original picture on *Arriba's* website.[103] The plaintiff argued that the defendant infringed the Digital Millennium Copyright Act.[104] The court reasoned that use of the images was not fair use, because the thumbnail pictures provided a link to a full size picture on *Arriba's* website (i.e. regarded as public display), thus making it unnecessary to visit the plaintiff's website wherein all of the original pictures were situated.[105] However, displaying only a thumbnail on *Arriba's* website fell under the fair use doctrine regardless of the defendant's copyright violation.[106] Despite the fact that certain categories of PII could be possibly protected under different branches of property law, especially in the case of intellectual property rights, granting general property rights in personal data is constitutionally challenging[107] on account of one crucial factor; 'property is not inherent in information'.[108] Even if personal data was protected by intellectual property rights, it would significantly hinder the free flow of information due to vast increase in new and novel property rights coming into existence on a daily basis - licensing would be painstaking and overall counterproductive to societal development in its entirety (e.g. interference with public goods such as research databases).[109]

Apart from property rights, reasoning behind the idea of information becoming public when voluntarily provided to a third party in case *Miller* is rather controversial. According to the precedent in a hypothetical situation any category of information could be regarded as public, if the condition of knowingly providing personal information to a third party is fulfilled. For example, if one makes a transaction in Google play store it is necessary to provide credit card

[102] United States Court of Appeals, Ninth Circuit, 336 F.3d 811, *KELLY v. ARRIBA SOFT CORP.* (2003)
[103] Id.
[104] Id.
[105] Id.
[106] Id.
[107] supra note 94, p.1141
[108] Einer Elhauge, The Fragmentation of U.S. Health Care: Causes and Solutions 1st Edition, March 22, 2010, p.195
[109] Id.

information in order to purchase a product. Such information required in the completion of a commonplace transaction would be considered having no expectation of privacy whatsoever under the 4t amendment, if the precedent set in *United States v. Miller* is followed literally, even though the credit card information is only exposed to Google and the transaction is recorded in a bank statement (i.e. not exposed to public per se). However, it cannot be denied that in a legal sense it is more than reasonable that information can be obtained by government agencies without infringing privacy rights in e.g. criminal investigations or audits. Casting personal information automatically in the category of non-personal information in consequence of disclosing data with a third party is still an incorrect rationale. Luckily, and at the same time unfortunately, the SCOTUS has been fairly inconsistent in the application of *United States v. Miller*. As an example in *Ferguson v Charleston* (2001),[110] a case involving a drug testing policy with respect of pregnant women who were suspected of drug abuse and patients of the Medical University of South Carolina, led to a decision inconsistent with precedent *United States v. Miller* (1976).[111] The drug screening carried out by employees of the hospital did not obtain an informed consent from the pregnant women and any subsequent data indicating positive drug abuse was provided to a local police force in order to criminally prosecute them.[112] The ten women who got arrested because of testing positive on the drug test, pursued a lawsuit against the City of Charleston and claimed that their constitutional rights had been violated.[113] Although the respondents argued for their actions being benign and for a common good (i.e. not mischievous in any aspect), the SCOTUS reasoned that the pervasive participation of the police and lack of an informed consent regarding the drug policy employed by the hospital deprived the defendants of their protection afforded under the 4th amendment.[114]

The above-named case therefore expresses that information voluntarily provided to another party does not automatically categorize such kind of data under title "public information" or "no reasonable expectation of privacy". Even Associate Justice Sotomayor of SCOTUS has stated:[115] "information voluntarily disclosed to third parties should not divest expectation of privacy and the precedent set in *United States v Miller* is ill suited to the digital age." In *Griswold v. Connecticut*

[110] U.S. Supreme Court, 532 U.S. 67, FERGUSON et al. *v.* CITY OF CHARLESTON et al. (2001)
[111] supra note 53, p.263
[112] Id.
[113] supra note 103
[114] Id.
[115] supra note 53, p.264

(1965)[116] it was reasoned that although certain fundamental rights (e.g. privacy) are not explicitly mentioned in any of the amendments, it does not mean that such fundamental rights cannot be protected under the constitution. Justice Goldberg cogently stated that 'deep rooted rights' in our society must be protected and abnegation of constitutional protection for rights like privacy cannot be justified on the basis of absent explicit terms in the constitution - depriving protection of basic rights on such grounds is contrary to the ninth amendment.[117] Taking into account all of the cases and U.S. Supreme Court's reasoning stated above, it is clear that privacy is protected in a diversified manner under the constitution. The inconsistencies in interpretation of reasonable expectation of privacy exacerbates the constitution's credence pertinent to data privacy. Still, it should be noted that resorting to the constitution in privacy issues is only viable in state actions as the constitution regulates exclusively governmental conduct (i.e. public matters) and not matters of private citizens or corporations (i.e. private sector).[118] The constitution does not proscribe 'deprivation of constitutional rights' being wholly ascribed to private conduct.[119] Only in circumstances wherein the state is deeply involved in a situation, where private conduct infringes constitutional values, the state can be held responsible for violating the constitution.[120] Under the aforesaid circumstances private behavior is also required to comply with the constitution, which is not the case in pure private conduct lacking salient involvement of state agencies.[121] The SCOTUS has stated that without a state action, no matter how grave or wrong a private conduct might be, the constitution cannot be resorted to as a shield.[122] In private sectors terms this means that legal problems emanating from right to privacy are left to be regulated under federal or state laws. Even if a case has elements of constitutional value, but is handled by a federal court, the last resort rule shall be applied. Accordingly, 'a federal court should not rule on a constitutional issue if the case can be decided on a non-constitutional basis'.[123] The last resort rule reifies the SCOTUS's standing with regard to state actions and the constitution's relationship with matters belonging into the private sector.

4.1.2 SCOTUS, Big Data and *Spokeo, Inc., Petitioner v. Thomas Robins* (2016)

[116] U.S. Supreme Court, 381 US 479, GRISWOLD V. CONNECTICUT (1965)
[117] Mark Niles, Ninth Amendment Adjudication: An Alternative To Substantive Due Process Analysis of Personal Autonomy Rights, 48 UCLA L. REV. 85 (2000), p.87, footnote 4
[118] Erwin Chemerinsky, Rethinking State Action, 80 *Northwestern University Law Review* 503-557 (1985), p.507
[119] Id., p.508
[120] Id.
[121] Id.
[122] Id., p.508-509
[123] 35 B.C. L. Rev. 1106, p.1004

How the SCOTUS will deal with cases involving only matters of Big Data concerning the collection of PII, as the 4th amendment does not apply to utilization of data, is a big question mark due to scarce constitutional case law in this respect. Yet, one recent case involving questions in relation to BD was partly addressed by the SCOTUS in 2016; *Spokeo, Inc., Petitioner v. Thomas Robins*[124]. Spokeo is a data broker company offering a web based 'people search engine' which provides particular information about various persons (data subjects) after typing in a person's name, a phone number, or an e-mail address.[125] The search system in question is based on a multitude of different databases.[126] The case in question concerned a grievance owing to incorrect PII regarding plaintiff *Thomas Robins*. After the plaintiff found about that an incorrect profile was made about him ('consisting of home address, phone number, marital status, approximate age, occupation, hobbies, finances, shopping habits, and musical preferences') he proceeded to file a class action lawsuit against Spokeo.[127] Initially the case was dismissed by the central district court of California owing to a lack of standing, but was picked up by the ninth circuit (Court of Appeals) and referred to the SCOTUS.[128] Mr.*Robins* argued that not only other's statutory rights were violated, but his statutory rights were also violated.[129] *Robins* claimed that the handling of his credit information was a personal interest of individual nature, not a collective one, and that his employment prospects were harmed due to the inaccurate data represented in the Spokeo search engine.[130] According to the arguments set forth by *Robins*, the appeals court held that there was an adequately alleged injury, which is a prerequisite for a standing. Nevertheless, the SCOTUS noted the ninth circuit court's analysis being incomplete.[131] Because *Robins* invoked to the FCRA (Fair Credit Reporting Act) he had the burden of proof establishing that an actual injury was suffered; the cause of the injury could be traced back to actions of the defendant (i.e. Spokeo); and a redress was most likely to grant a decision in favor of the plaintiff.[132] The SCOTUS in its opinion to the ninth circuit court maintained that an injury must be *de facto* particular and concrete, both of these factors were not taken into account by the appeals court.[133] It was also remarked by the SCOTUS that *Robins* could not bring the case into a federal court under Article III of the constitution, if his

[124] U.S. Supreme Court, 578 U. S. ____ (2016), *Spokeo, Inc., Petitioner v. Thomas Robins* (2016)
[125] Id.
[126] Id.
[127] Id.
[128] Id.
[129] Id.
[130] Id.
[131] Id.
[132] Id.
[133] Id.

allegation were merely based on a procedural violation with respect of the FCRA (e.g. "an incorrect zip code is unlikely to cause concrete harm or pose material risk of harm").[134] The SCOTUS took no positions on the ninth circuit court's final decision and its correctness, however, the case was vacated and remanded by the SCOTUS.[135]

Before the SCOTUS gave its opinion on the case, there were many concerns how the outcome of the case would affect consumer privacy altogether. Troutman Sanders, an American law firm, wrote on their website in 2015 that the end results of the case will be figuratively a two-way street; either no-damage class actions based on a technical liability will become viable; or plaintiffs will be required to plead and substantiate concrete harm.[136] If the latter takes place, class action lawsuits in relation to consumer privacy will become extremely cumbersome for parties whose expectation of privacy is at stake.[137] Even the Electronic Privacy Information Center (EPIC) filed an *amicus curiae* brief in 2015 in which EPIC asserted that ruling in favor of Spokeo would lead to degradation of protection guaranteed under the FCRA and individual's ability to prevent misuse of personal information would be distinctly undermined.[138] It was also pointed out in the brief that if the SCOTUS accepts Spokeo's argument (i.e. violation of a federal law is not sufficient enough to gain standing pursuant to article III because of a lack of proof corroborating consequential harm) the deterrent effect in federal laws will be limited to a degree which to same extent increases overall risk of data breaches.[139] Along with the FCRA, other categories of sensitive information regulated under various federal laws would be exposed to misuse such as 'The Cable Communications Policy Act, The Driver's Privacy Protection Act, The Electronic Communications Privacy, The Fair Debt Collection Practices Act, The Fair and Accurate Credit Transactions, The Right to Financial Privacy Act, The Telephone Consumer Protection Act and The Video Privacy Protection Act'.[140] And those are just to name a few examples from a bundle of Acts constituting the U.S. data privacy regime on a federal level. Another grievance regarding the Court's opinion was an example of the use of zip code data. Data & Society: Points wrote on

---

[134] Id.
[135] Id.
[136] David N. Anthony, Alan D. Wingfield, Julie D. Hoffmeister and Virginia Bell Flynn, "Standing on Thin Air: Spokeo, Inc. v. Robins", Troutman Sanders LLP, 11.03.2015. <https://www.troutmansanders.com/standing-on-thin-air-spokeo-inc-v-robins-11-03-2015/>(29.1.2017)
[137] Id.
[138] Marc Rotenberg, Alan Butler, T. John Tran, "Brief of Amici Curiae Electronic Privacy Information Center (EPIC) and Thirty Two Technical Experts and Legal Scholars in Support of Respondent", September 8, 2015, p.20-21
[139] Id., p.22
[140] Id., p.21

their homepage that the Supreme Court's imagination and knowledge in relation to data science is lacking badly as zip codes commonly play an important role in different algorithms that are used to determine, for example, consumers' affluence.[141] Respectively, FTC consumer report published in 2016 expressed its concern towards online retailers engaging in price discrimination via utilization of zip code data.[142] Even though the case was not about zip code data, and was merely mentioned in order to second a rationale, it is evident that judges need to acknowledge that seemingly innocuous data has inherent potential to cause concrete harm under particular circumstances.[143]

Unfortunately case Spokeo was vacated and remanded, which means the final decision and its outcome will be clear after the ninth circuit court completes a "do-over". 'The opinion of the SCOTUS is regarded as major victory for companies dealing with consumer data' because a loss for Spokeo would have most likely set off a chain reaction of class action lawsuits bearing a potential of billions of dollars in actual damages.[144]

4.2 Federal Statutes vis-à-vis Big Data from a Case Law Perspective

Data privacy on a federal level is regulated by multiple sector specific laws, which focus on specific categories of data (e.g. FCRA - consumer reports, or Privacy Act - government collection and use of data).[145] Due to the sector specific nature of the federal data privacy regime, a single comprehensive federal law which would take into account more than a few data categories does not exist.[146] This disunity of federal privacy statutes inevitably complicates the interpretation of privacy protection provided on a federal level and has the potential creating a legal vacuum in respect of current data practices, especially in the case of BD. The evident problem in the sector specific approach can be ascribed to its direct specificity and lack of comprehensiveness. For example, a private company that does not fall into a specific industry category, or when the personal data in question is not the type of data covered by a particular federal statute, the sectoral

[141] Kiel Brennan-Marquez, "The Supreme Court's Big Data Problem", Data & Society: Points, 29.06.2016. <https://points.datasociety.net/the-supreme-courts-big-data-problem-9401fa88a3e0#.hllsyg5il>(7.2.2017)
[142] Id.
[143] Id.
[144] Jeff John Roberts, "Supreme Court Rejects Privacy Claim in Data Broker Case", Fortune, 16.05.2016.<http://fortune.com/2016/05/16/supreme-court-spokeo-decision/>(7.2.2017)
[145] Clark D. Asay, Consumer Information Privacy and the Problem(s) of Third-Party Disclosures, 11 Nw.J. Tech.& Intell.Prop.321 (2013). p.325, 336
[146] supra note 7

law under such circumstances will be inapplicable to the business entity and to the type of information employed altogether.[147] Moreover, the sectoral approach can be exploited via 'disruptive technology' or by stretching the norms concerning statutory interpretation (i.e. strained interpretation of a law).[148] Case *Kehoe v. Fidelity Federal Bank & Trust* has been regarded as a prime example of what can happen when a federal statute is circumvented via strained interpretation.[149] In the case, *Fidelity Federal Bank & Trust* bought 565500 individuals personal data from the Florida Department of Highway Safety and Motor Vehicles for marketing purposes.[150] The *Fidelity Federal Bank & Trust* argued that because the state of Florida had not amended its law according to the Driver's Privacy Protection Act, informed consent for the release of the purchased information was not required.[151] The SCOTUS refused to review the case and the final decision resulted in a multimillion dollar settlement due to other class action lawsuits pertaining to same legal issue in the state of Florida.[152] Although *Kehoe* resulted in substantial settlement, marketers are still willing to get hold of driver data hold by DMVs.[153] [154]

Another great example concerning the sectoral approach and its weaknesses when faced by "new technologies" is case *Deacon v. Pandora Media, Inc*. The case involved a legal dilemma of whether Pandora Media Inc. (an internet radio service) could be held liable for disclosing music listening habits and history to other users, including friends in Facebook, and if such conduct was against Michigan's Video Rental Privacy Act.[155] Plaintiff Peter Deacon filed a class action lawsuit against the Pandora Media Inc. by claiming that his and other Michigan based users' statutory rights had been violated due to improper disclosure of the above-mentioned listening data.[156] Nonetheless, the case was dismissed due to the fact that the Video Rental Privacy Act (VRPA) applies only to selling, renting or lending of sound recordings, and because the defendant streamed music to the plaintiff's computer such conduct fell outside the scope of the VRPA.[157] Although

---

[147] supra note 138, p.325
[148] Hoofnagle, Chris Jay, New Challenges to Data Protection Study - Country Report: United States, January 20, 2010, p.21
[149] Id.
[150] U.S Supreme Court, 547 U. S. ____ (2006), *Kehoe v. Fidelity Federal Bank & Trust* (2006)
[151] Id.
[152] Id.
[153] supra note 141
[154] Steve Orr, "Is your DMV data safeguarded properly?", Rochester (N.Y.) Democrat and Chronicle, 17.03.2015.<http://www.democratandchronicle.com/story/news/2015/03/16/dmv-data-security-sunshine-week-new-york-privacy/24846627/>(9.2.2017)
[155] United States District Court, Northern District of California, Case No: C 11-04674 SBA, *Deacon v. Pandora Media, Inc.* (2012)
[156] Id.
[157] Id.

the case did not directly rely on the federal Video Privacy Protection Act (VPPA) and focused on the State of Michigan version of it, still the sector specific nature of the VRPA was the main reason why the plaintiff's claim overall stymied. It was remarked earlier that a private company that does not fall into a specific industry category, or when the personal data in question is not the type of data covered by the federal statute, the sectoral law under such circumstances will be inapplicable to the business entity and to the type of information employed altogether.[158] The above-said is exactly what happened in *Deacon v. Pandora Media Inc*.

In *re: Hulu Privacy Litigation* a decision was made in stark contrast to the end result of *Deacon v. Pandora Media Inc.* A putative class action lawsuit was filed against the video streaming service Hulu for an alleged and wrongful disclosure of PII to data tracking company called 'comScore' and the social network company Facebook under the VPPA.[159] Hulu argued that it did not violate the VPPA because it only disclosed anonymous user IDs; it did not disclose the information knowingly; lastly Facebook's terms of use permitted the disclosure and thus Hulu users who use Facebook automatically approved disclosure of the user's video choices.[160] The court granted a summary judgment motion to the comScore disclosures due to its fully anonymous nature, but denied summary judgment motion with respect of Facebook as disclosed video names were linked to Facebook user accounts via Facebook's like button feature.[161] Moreover, it was not clear if Hulu *de jure* knowingly disclosed PII or not.[162] The court also maintained that Hulu could not possibly escape the VPPA by claiming that their model of business could not be considered as a video tape service provider, because the very definition of a video tape service provider pursuant to 18 U.S.C. § 2710 (a)(4) includes wording "similar audio visual materials".[163] And users of services provided by Hulu can be regarded as consumers under the VPPA.[164] The district court dismissed the plaintiff's second amended complaint with prejudice in 2015 and granted Hulu's motion for summary judgment after finding that there was not enough evidence corroborating that Hulu knowingly disclosed any PII from the very beginning.[165] It was also pointed out that another significant factor in the court's final decision was the plaintiffs' incapability of establishing any

[158] see footnote 138, p.325
[159] United States District Court, Northern District of California, Case No: C 11-03764 LB, *In Re: HULU Privacy Litigation* (2012)
[160] Id.
[161] Id.
[162] Id.
[163] Id.
[164] Id.
[165] United States District Court, Northern District of California, Case No: C 11-cv-03764 LB, *In Re: HULU Privacy Litigation* (2015)

material fact that would have proved Hulu's awareness in relation to activities carried out by the Facebook.[166] To put it plainly, the plaintiffs failed to show that Hulu might have actually known that the Facebook combined Facebook user's identity (i.e. c_user cookie) with the video titles embedded into Hulu's watch page URL in order to produce PII.[167] Hulu convincingly stated that the watch page URL and c_user cookie alone cannot constitute PII under the VPPA.[168] In terms of private companies that employ BD, the decision rendered in *In Re: HULU Privacy Litigation* can be interpreted in multiple ways. Firstly, if a company has no knowledge of leaking identifiable information to a third party, the company in question is unlikely held responsible for such conduct. Secondly, plaintiffs have to overcome a significant burden of proof in order to establish that a company has violated one's right to privacy. Thirdly, the definition of personally identifiable information varies and it is dependent on the sector specific federal statute. Lastly, if plaintiffs can prove that a company has even a tiny bit of knowledge that the data leaked to a third party led to a discovery of PII, then it is possible that the company can be held liable. Dominique Shelton, partner in law firm Alston & Bird LLP, remarked that any company aware of the decision rendered in *In Re: HULU Privacy Litigation* could be used by creative plaintiffs in order to assert companies' "implied knowledge".[169] Still, it should be noted that most of the privacy focused federal statutes do not afford private right of action.[170]

If an individual wants to file a lawsuit against a private company under the sector specific federal statutes regulating privacy, class action lawsuits are the best option available in most circumstances.[171] Class actions also serve as an alternative method to government or industry specific self-regulation.[172] If an industry is not motivated or properly organized to ensure that all of its members will comply with self-regulation, the outcome of implementing self-regulation will be ineffective.[173] When a federal statute does not provide the possibility to private enforcement, consumers have to resort to federal, government or state agencies, such as the consumer protection agency FTC in order to enforce statutory rights.[174] If it is assumed that costs in association with

---

[166] Id.
[167] Id.
[168] Id.
[169] Allison Grande, "Hulu's Win Won't Halt Video Privacy Class Actions", Law360, April 1, 2015.<https://www.law360.com/articles/638399/hulu-s-win-won-t-halt-video-privacy-class-actions>(15.2.2017)
[170] Françoise Gilbert, Catherine D. Meyer, Denise Olrich, Paul T. Smith, Roy G. Weatherup, Privacy Compliance and Litigation in California: 2016 Update, September 2016, p.16
[171] Janet Cooper Alexander, An Introduction to Class Action Procedure in the United States, Presented Conference: Debates over Group Litigation in Comparative Perspective, Geneva, Switzerland, July 21-22, 2000., p.1
[172] Id.
[173] Id. p.1-2
[174] Id. p.2

collection and storage of data decreases significantly over time due rapid technological development, small newcomer companies can get access to BD handling techniques in the near future.[175] Respectively, in that kind of hypothetical situation, a private right of action will not be a certain option in relation to small newcomer companies, if only a few limited sector specific federal statutes allow a private party to bring a lawsuit before the court. Under the aforesaid hypothetical situation it is reasonable to presume that consumer protection agencies will be overburdened by privacy related complaints as the amount of companies with data handling capabilities increases significantly. It has been also noted that especially consumer protection agencies do not currently have enough resources to detect every violation nor the resources to prosecute all of the violations.[176] And consumer protection agencies rarely seek actual compensation for consumers.[177] Regardless, including a private right of action in a statute has been proven problematic due to distinct overlap with the ability of consumer protection agencies to exercise their primary jurisdiction created for the enforcement of specific statutes,[178] such as the FTC and its responsibility in relation to enforcement of the FTC Act.

4.2.1 The two baseline statutes

The FCRA and Privacy Act can be regarded as two pieces of legislation which constitute the very core of the federal data privacy regime,[179] even though the Privacy Act only applies to federal government (i.e. nor state nor local) agencies and to private sector companies maintaining records for the government.[180] Therefore, scope of the Privacy Act is limited to actions that are carried through a contractual relationship between a federal government agency and a private company.[181] This leaves consumer reporting agencies, data brokers and private companies engaging in BD outside the Privacy Act's purview, unless information is directly transferred from a federal agency to the contracted private company.[182] One major grievance in this regard is that, for example, data brokers can freely gather as much information as possible without the worry of 'triggering any provisions contained in the Privacy Act'.[183] Although most of the American companies do not

[175] supra note 3, p.25
[176] supra note 168
[177] Id.
[178] James T. O'Reilly, Deregulation and Private Causes of Action: Second Bites at the Apple, 28 Wm. & Mary L. Rev. 235 (1987), p.242
[179] supra note 19, p.3
[180] Id. p.9
[181] Id.
[182] Id.
[183] Id.

acknowledge the principle of proportionality in data collection, to some extent the principle is contained in the Privacy Act.[184] Pursuant to the Act, federal systems of records should only contain information which is needed in order to carry out activities specifically assigned to the federal agency.[185] In addition, pertaining to determination of granting federal benefits, agencies are obligated to collect information directly from the data subject, if such collection can be regarded as potentially detrimental in association with the expected outcome.[186] This very clause in the Privacy Act is regarded as the quintessential limitation rule within the U.S data privacy regime.[187]

In *Federal Aviation Administration v. Cooper* (2012) a private right of action was instantiated under the Privacy Act,[188] which is not viable in respect of most of the federal statutes regulating matters of privacy. The case in question concerned a commercial pilot who withheld his true state of health from the FAA for decades - the respondent did not disclose he had HIV.[189] When the respondent's condition deteriorated, he applied to the social security administration (SSA) and received long-term disability benefits as a consequence of being HIV positive.[190] The FAA's parent agency DOT (department of transportation) opened a joint criminal investigation with the SSA in order to catch unhealthy individuals who had acquired FAA certifications under false pretenses.[191] The DOT provided the SSA with a list containing names of all certified pilots, and the SSA in turn provided the DOT with a list containing names of the pilots who had received disability benefits.[192] Eventually it was unearthed that Mr. Cooper had failed to fully disclose his medical condition, HIV positive.[193] He plead guilty and his pilot license was revoked. Subsequently, Cooper filed a lawsuit against the FAA, DOT and SSA by claiming that his right to privacy was violated under the provisions of the Privacy Act.[194] The Act allows an aggrieved party to sue for actual damages, which can be construed as a private right of action.[195] Cooper claimed that he had suffered mental and emotional distress because of an unlawful disclosure of the medical information forwarded to the DOT.[196] The district court and the ninth circuit court admitted that

[184] supra note 141, p.24-25
[185] Id.
[186] Id., p.25
[187] Id.
[188] U.S. Supreme Court, 566 U. S. ____ (2012), *Federal Aviation Administration v. Cooper (2012)*
[189] Id.
[190] Id.
[191] Id.
[192] Id.
[193] Id.
[194] Id.
[195] Id.
[196] Id.

the government agencies involved in the case had indeed violated the Privacy Act, but the SCOTUS remarked that under the Privacy Act mental or emotional distress cannot be unambiguously regarded as actual damages per se.[197] Thus, the Privacy Act did not authorize awarding damages for such harm experienced by the respondent.[198] To the same extent, the SCOTUS stated that because the Privacy Act does not allow recovery of non-pecuniary damages, the Act did not deprive the federal government of its 'sovereign immunity waivers' in the context of mental or emotional distress.[199] That is to say, if a respondent cannot substantiate actual monetary or economic loss in association with a privacy violation, a federal agency or a contracted private company maintaining a system of records for the former are excluded from any liability under the Privacy Act. This case reaffirms a particular "keynote" in privacy litigation in context of the research, at least, on a federal level - claimants have a relatively high *onus probandi* to overcome and ultimately an actual tangible loss is a fundamental factor serving as the main basis for a convincing claim regarding loss of privacy. Regardless, as the Privacy Act only applies to federal government (i.e. nor state nor local) agencies and to private sector companies maintaining records for the government,[200] any further deliberation of the Privacy Act's privacy protection in relation to the private sector domain is otiose.

The second core federal statute is the FCRA and it is directly applicable to companies operating within the private sector. More specifically, it applies to consumer reporting agencies (CRAs), which by the very definition are persons who regularly collect information about consumers with the intention of selling or rendering consumer reports to third parties.[201] Albeit the definition of a consumer reporting agency under the FCRA is dependent on the usage of the information collected.[202] A consumer report can be any form of communication containing a consumer's personality, character or overall reputation which is used, for instance in insurance underwriting, credit evaluation and pre-employment screening.[203] According to the FCRA, CRAs are required to maintain maximum accuracy of the information compiled, grant consumers access to their PII and provide them with the opportunity to rectify any mistakes in the information contained in a consumer report.[204] If an individual wants to rectify wrong information provided to a creditor (i.e.

[197] Id.
[198] Id.
[199] Id.
[200] supra note 167
[201] supra note 19, p.7
[202] Id.
[203] Id.
[204] Federal Trade Commission Report, Big Data: A Tool for Inclusion or Exclusion?, January 2016, p.13

third party) by the CRA, the aggrieved consumer must firstly notify the CRA and hope that the notification also reaches the creditor.[205] If the creditor is not aware that the validity of particular information concerning a specific consumer has been disputed by the consumer, there will be no private right of action.[206] If a consumer wants to file a lawsuit against the creditor, it is necessary for the consumer to delineate 'the interaction between the creditor and the CRA' in respect of communication concerning the disputed data.[207] If the Creditor is not notified, the creditor does not have to investigate whether the information is truly false or not.[208] If the consumer disputes information directly provided by the creditor, the latter has to inform the CRA that the information in question has been disputed.[209] Regardless of the grievance, the consumer cannot force the creditor to inform the CRA, only federal enforcement authorities or state agencies are capable of doing this under the FCRA.[210] The FCRA contains two pitfalls: (I) consumers cannot privately enforce statutory rights concerning the duty of accuracy when such rights has been violated by the creditor; (II) if a consumer wants to rectify wrong information provided to a creditor by the CRA via private right of action, the aggrieved consumer must able to present facts which are required 'to allege a plausible claim' (i.e. communication between the creditor and the CRA about the disputed information), though these prerequisite facts are often possessed by the creditor instead of the consumer.[211]

It has been also argued that a literal interpretation of the definition consumer report has a chance to render the FCRA inapplicable in circumstances wherein information is used in an unauthorized manner and mainly for purposes not listed in the FCRA (e.g. fraud).[212] But the FTC has established that data brokers collecting "non-traditional information" such as social media data, can be held subject to rules prescribed in the FCRA.[213] A direct example of the aforesaid was reified in *United States v. Spokeo Inc.* (2012),[214] the case concerned the very same company mentioned in Chapter 4.1.2.

[205] Jeffrey Bils, 61 UCLA L. Rev. Disc. 226, Fighting Unfair Credit Reports: A Proposal to Give Consumers More Power to Enforce the Fair Credit Reporting Act (2013), p.232
[206] Id.
[207] Id., p.234
[208] Id.
[209] Id., p.233
[210] Id.
[211] Id., p.242
[212] supra note 19, p.7
[213] supra note 192
[214] Id.

Case *United States v. Spokeo Inc.* was handled by the United States District Court for the Central District of California and brought before the court by the state on behalf of the FTC.[215] Under section 5(a) of the FTC Act, the commission is given statutory authority and responsibility to enforce prohibitions concerning unfair or deceptive trade practices.[216] The FTC's complaint maintained that Spokeo violated many of the provisions contained in the FCRA and carried out activities contrary to the section 5(a) of the FTC Act while selling consumer profiles to human resources departments in various companies.[217] The plaintiff claimed that Spokeo failed to maintain procedures laid down in the FCRA, which specifically require any CRA to ensure that consumer reports provided to a third party will not be used for an impermissible purpose; third parties to which a consumer report is provided must also identify themselves to the CRA; the CRA has to make a reasonable effort in order to verify real identify of the third party and to further certify the main purpose for which a consumer report is sought after; and to take reasonable steps in order to maintain maximum accuracy of the information contained in a consumer report.[218] The plaintiff claimed that Spokeo failed to abide by the notification requirements clearly stated in the FCRA.[219] According to this user notice obligation, a user of a consumer report must notify the particular consumer if he or she "is subject of an adverse action (e.g., denial of employment) based in whole or in part on information contained in the consumer report".[220] As regards violations in relation to the FTC Act, Spokeo made false endorsement statements on their homepage and other technology websites by claiming that all of the posted comments were submitted by independent users of Spokeo (e.g. normal consumers) when in fact the endorsing comments were created and submitted by Spokeo employees and managers.[221] This conduct was captured under the FTC Act and held unfair and deceptive pursuant to Section 5(a).[222]

End result of the case led to a hefty settlement between the FTC and Spokeo - the "price tag" was a total sum of 800000$.[223] The FTC also stipulated in the settlement that Spokeo must refrain and

[215] United States District Court for the Central District of California, Case No. 2-12-cv-05001-MMM-SH, *United States v. Spokeo Inc.* (2012)
[216] Id.
[217] Id.
[218] Id.
[219] Id.
[220] Id.
[221] Id.
[222] Id.
[223] FTC Press Releases, "Spokeo to Pay $800,000 to Settle FTC Charges Company Allegedly Marketed Information to Employers and Recruiters in Violation of FCRA", June 12, 2012. <https://www.ftc.gov/news-events/press-releases/2012/06/spokeo-pay-800000-settle-ftc-charges-company-allegedly-marketed>(25.2.2017)

is barred from any subsequent FCRA violations.[224] Furthermore, Spokeo is prohibited from posting comments which are not truly independent due to the Section 5(a) violation of the FTC Act.[225] When this case is contrasted to *Spokeo, Inc., Petitioner v. Thomas Robins* (2016), it is hard to fathom why the outcome of the latter case distinctly differs from the former, if the settlement clearly barred Spokeo from violating provisions of the FCRA. One of the main reasons for the unfortunate outcome in *Spokeo, Inc., Petitioner v. Thomas Robins* (2016) was the lack of preponderance of evidence which was required in order to prove that Robins' suffered an actual injury.[226] It was also argued in the case that the statutory requirement in the FCRA, which lays down a rule to guarantee maximum accuracy of information in relation to consumer reports, could have the potential to create a private right.[227] But it was also remarked that Robins was seeking a redress specifically connected to misinformation presented about him,[228] unlike in *United States v. Spokeo Inc.* where the redress concerned consumers at large. The juxtaposition of the two above-mentioned Spokeo affined cases indicate that enforcement of statutory rights is extremely cumbersome even when there is a high probability that the defendant has violated federal provisions aimed for the protection of privacy, if the sought redress would only benefit one individual instead of a large group of people (i.e. consumers as a whole). As a side note, it could be also argued in the light of the Spokeo related cases that a complaint filed by the FTC bears significant "sway" when compared to class action lawsuits initiated by ordinary consumers. Though, it is noteworthy to point out that this can be partly ascribed to the FTC's "watchdog" status amongst other federal agencies, due to the enforcement responsibilities assigned to the FTC in respect of the FTC Act and due to the lack of private right of action in most of the federal statutes.

4.2.2 FTCA in light of agency settlements

Section 5 of the FTC Act covers unfair and deceptive trade practices and is solely enforced by the FTC due to exclusion of the right to private action. Enforcement cases regarding unfair or deceptive trade practices are commonly settled between the FTC and defendant.[229] It is also

[224] Id.
[225] Id.
[226] 130 Harv. L. Rev. 437, *Leading Case :* 136 S. Ct. 1540 (2016), November 10, 2016.<http://harvardlawreview.org/2016/11/spokeo-inc-v-robins/>(25.2.2017)
[227] Id.
[228] Id.
[229] supra note 6, p.7

common that the defendant is not required to admit the alleged wrongdoing, if a settlement is reached.[230] However, the FTC frequently imposes compliance burdens to companies, if the company in question carries out activities contrary to rules prescribed in the FTCA.[231] When a company is ordered to implement a program aimed to improve its data privacy practices it will be also subject to periodic audits carried out by independent parties.[232] These audits last for the whole settlement period, which can be as long as 20 years. If the defendant violates any of the provisions contained in the settlement during the settlement period, the FTC will impose substantial fines.[233] The significance of the Section 5 in data protection is further consolidated in *FTC v. Wyndham Worldwide Corp.,*[234] the case established that specific data security breaches could be held as unfair practices under Section 5. Thus, the FTC has authority to bring enforcement actions against companies whose incapability to protect sensitive data causes substantial harm to consumers.[235]

The FTC employs different methods for determining if a certain practice can be deemed unfair or deceptive.[236] In the fairness test the FTC conducts a cost-benefit analysis in order to decide whether certain behavior causes substantial and avoidable injury to consumers.[237] If the injury cannot be counterbalanced by consumer benefits, the practice under scrutiny will be regarded as unfair.[238] A large injury affecting a small number of consumers can constitute substantial injury and a small injury affecting a large number of consumers can be held equal to substantial injury as well.[239] Nonetheless, it has been remarked that in the field of data protection measuring actual injuries concerning consumers is not an easy task due to low threshold in relation to risks bearing probability of substantial injury.[240] And when small injuries are addressed on an individual basis, the quantifiability of such injuries is challenging.[241] But the FTC has construed any practice leading to loss of autonomy or choice with respect to consumers bears a possibility that could cause substantial injury.[242] The quantification of deceptive trade practices differs to a large degree

[230] Id.
[231] Id.
[232] Id.
[233] Id.
[234] 129 Harv. L. Rev. 1120, *FTC v. Wyndham Worldwide Corp.,* February 10, 2016.<http://harvardlawreview.org/2016/02/ftc-v-wyndham-worldwide-corp/>(25.3.2017)
[235] Id.
[236] supra note 8, p.206
[237] Id.
[238] Id.
[239] Id.
[240] Id., p.207
[241] Id.
[242] Id.

in contrast to the cost-benefit analysis utilized in association with unfair trade practices. If a company does follow its own formulated privacy policies, the FTC cannot hold questionable activities carried out by the company as deceptive.[243] In such circumstances the FTC has to substantiate that the practice under scrutiny is unfair.[244] In *Wyndham* the FTC relied on the unfair trade practice prong,[245] instead of basing the claim solely on deceptive trade practice.

Even if a private company's conduct in relation to collection, storage or disclosure of data is not directly regulated by specific data privacy or security laws, it may still be subject to prosecution initiated by the FTC or state Attorney Generals.[246] When companies engage in handling of PII in conjunction with inadequate privacy and information protection there is a high chance that the company devoid of adequate data protection measures will be held liable to damages,[247] especially when faced by the FTC's consent orders due to conduct deemed contrary to Section 5 of the FTCA. The FTC's enforcement case law is abundant and numerous established companies have been prosecuted by the FTC for privacy violations.[248] For example, in a recent case *FTC, Attorney General of the State of New Jersey and Director of the New Jersey Division of Consumer Affairs v. VIZIO, INC. and VIZIO Inscape Services, LLC* a well-known American flat-screen TV manufacturer paid a settlement worth of 2.2$ million (including a payment of $1.5 million to the FTC and $1 million to the New Jersey Division of Consumer Affairs) for obtaining viewing data on 11 million consumer televisions without an express consent.[249] VIZIO was also ordered to delete all of the data collected before 1.3.2016 and to implement a data privacy program subject to biannual audits.[250] The defendant's conduct was held unfair and deceptive under the FTCA. In the same manner, many large private companies including Facebook, Google, Microsoft, Netflix et cetera have settled cases for privacy violations and in consequence of misleading consumers at large. In *FTC v. Snapchat Media, Inc.* the mobile application company famous for its video messaging platform was charged for deceiving consumers due to making false privacy protection

[243] Id.
[244] Id.
[245] supra note 230
[246] John K. Halvey, Barbara Murphy Melby, Business Process Outsourcing: Process, Strategies, and Contracts, 2nd Edition, April 2007, p.467
[247] Id.
[248] Id.
[249] FTC Press Releases, "VIZIO to Pay $2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions without Users' Consent", February 6, 2017.<https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it>(25.3.2017)
[250] Id.

promises.[251] Essentially, *Snapchat Media, Inc.* was not straightforward to its customer base about the real amount of personal data it collected and falsely maintained that necessary steps were taken in order to prevent misuse of PII.[252] The company in question was required to implement a privacy program subject to audits by independent privacy professionals for the period of 20 years.[253] Even data brokers have been held liable to damages by the FTC. For instance, in *FTC v. Sitesearch Corporation, dba LeapLab* the defendants violated the FTCA because of selling sensitive PII (social security numbers and bank account numbers) to illegitimate third parties.[254] The defendants bought payday loan applications and resold most of the information contained therein to parties who utilized the data for emptying consumers' bank accounts.[255] The defendants were found guilty of unfair trade practice and ordered to pay substantial damages, including total destruction of any consumer data in their possession.[256]

The FTCA has captured a multitude of violations regarding consumer privacy, especially under circumstances where a certain conduct or practice has not fallen into the purview of a sector-specific federal statute. Yet, there are still grievances regarding the general effectiveness of the FTCA. Section 5 of the FTCA only creates agency settlements.[257] In contrast to normal litigation, the FTC enforcement cases do not articulate what type of conduct is unlawful and lawful.[258] Implementation of Section 5 can only render a decision which can be held unfair and deceptive or neither of the two. Furthermore, settlements are not regarded as precedents by the FTC - settlements are devoid of any precedential value.[259] Another grievance is that the party at fault does not have to admit guilt after entering into a settlement with the FTC. This further exacerbates and dilutes much needed transparency as regards collection, storage and handling of PII in the era of datafication. If a clear delineation is not made between unlawful and lawful conduct, one cannot determine definitively the rights of data subjects and controllers in the light of past or future agency

[251] FTC Press Releases, "Snapchat Settles FTC Charges That Promises of Disappearing Messages Were False", May 8,2014.<https://www.ftc.gov/news-events/press-releases/2014/05/snapchat-settles-ftc-charges-promises-disappearing-messages-were>(26.3.2017)
[252] Id.
[253] Id.
[254] FTC Press Releases, "Data Broker Defendants Settle FTC Charges They Sold Sensitive Personal Information to Scammers", February 18, 2016.<https://www.ftc.gov/news-events/press-releases/2016/02/data-broker-defendants-settle-ftc-charges-they-sold-sensitive>(27.3.2017)
[255] Id.
[256] Id.
[257] Rybnicek, Jan M. and Wright, Joshua D., Defining Section 5 of the FTC Act: The Failure of the Common Law Method and the Case for Formal Agency Guidelines (September 15, 2014). 21 (5) George Mason Law Review, 1287 (2014), p.1305
[258] Id.
[259] Id.

settlements. The FTCA has also been criticized for not providing consumers a private right of action against perpetrators violating the Act.[260] This specific grievance stems from the fact that state consumer protection laws do not have as broad enforcement capabilities as the FTC.[261] Without a private right of action; consumers cannot receive the same redress available to the FTC; enforcement of past FTC decisions is impossible; and consumers cannot file for an injunctive relief.[262] The lack of private right of action is further highlighted by the sheer increase in the amount of so called "piggyback" class actions filed in recent years.[263] These class actions mirror earlier allegations made by the FTC and aim to convert an alleged violation of the FTCA into a private right cause of action, which is not possible.[264]

4.3 Lack of General Rules and State to State Divergence

U.S. data privacy legislation does not expressly define sensitive data, although federal statutes pay special attention to websites collecting data of children under the age of 13 (COPPA); information collected by financial institutions (GLB); health information collected by health care providers (HIPAA); and credit histories collected by CRAs (FCRA).[265] Personal data such as: 'name, residence address, e-mail, mobile phone number, income level, marital status, sex, and race' are not typically regarded as sensitive data and therefore not afforded protection under federal statutes.[266] As the U.S. does not have a dedicated data protection law, the definition of PII is dependent on the sector-specific statutes and regulations.[267] Mainly social security numbers, driver's license numbers and bank account numbers are conceived as sensitive PII.[268] In addition to lack of sensitive data categories, there is no general data retention limit concerning PII.[269] Service providers can retain data indefinitely and this practice is further bolstered by data mining

[260] Stephanie L. Kroeze, The FTC Won't Let Me Be: The Need for a Private Right of Action Under Section 5 of the FTC Act, 50 Val. U. L. Rev. 227 (2015), p.230
[261] Id., p.252
[262] Id., p.267-268
[263] John E. Villafranco and Daniel S. Blynn, Kelley Drye & Warren LLP, "The Case of the Piggyback Class Action", September 2012, p.22<http://www.kelleydrye.com/News-Events/Publications/Articles/The-Case-of-the-Piggyback-Class-Action>(29.3.2017)
[264] Id., p.24
[265] King, N. J. and Raja, V.T. (2013), What Do They Really Know About Me in the Cloud? A Comparative Law Perspective on Protecting Privacy and Security of Sensitive Consumer Data. Am Bus Law J, 50: 413–482., p.424-425
[266] supra note 266, p.445
[267] Rosemary P Jay, Hunton & Williams, Lisa J Sotto and Aaron P Simpson, Getting the Deal Through - Data Protection & Privacy 2015, Law Business Research Ltd 2014, p.209
[268] Id.
[269] Id.

activities aimed to a large extent for the pursuit of commercial revenue.[270] There are still laws that can indirectly limit retention of PII, such as the California Online Privacy Act.[271] The Act requires that organizations collecting PII online from California residents must provide data subjects with a privacy notice entailing information about the company collecting data and how the data will be used.[272] If a company materially changes use of the data initially stated in the first privacy notice without asking further consent or providing another notice, the company will be subject to unfair or deceptive trade practice.[273] California has also implemented "Shine the Light Law" which requires companies collecting PII from California residents to disclose if the data is used for direct marketing purposes and to which third parties the collected PII will be shared.[274] Data subjects also have the right to opt out of the aforesaid third party sharing.[275] Nonetheless, it should be noted that the California Online Privacy Act and the Shine the Light Law are only applicable to California residents and residents in other states are not necessarily provided with the same level of protection.

On a federal level there is no general breach notification law in place.[276] Many states have implemented statutes requiring companies to notify consumers in the event of a data breach, however, state data breach notification laws do not impose specific data security protocols.[277] Due to the aforesaid reason, if personal data is encrypted, companies are not necessarily obligated to report data breaches.[278] The state of California addressed the very issue by amending its civil code to require companies to report data breaches even if data is encrypted.[279] Commonly a data breach notification under the state notification laws is required only when a breach discloses residents' name and includes another sensitive data element.[280] The type of personal information triggering a breach notification in the event of an unlawful disclosure on state level is solely dependent on how the state *de jure* categorizes different data types. For example, in the state of California and

[270] supra note 26, p.585-586
[271] supra note 268
[272] Id.
[273] Id., p.210
[274] Id.
[275] Id.
[276] supra note 266, p.445-446
[277] Id.
[278] Id., p.446
[279] AGATA DZIEDZIC | US Privacy Analyst, "California: "Common sense" encryption amendment incorporated into breach notification law", DataGuidance, 29 September 2016.<http://www.dataguidance.com/usa-california-introduces-common-sense-data-breach-notification-amendment/>(4.4.2017)
[280] DLA Piper, Data Protection Laws of the World: United States, see p.3 of the handbook. <https://www.dlapiperdataprotection.com/index.html?t=law&c=US>(4.4.2017)

under its general breach notification statute; a username or email address in combination with a password or security question, medical information, health insurance information, and data obtained via an automated license recognition system are considered as personal information in addition to the common data elements like social security numbers, identity document card numbers (including driver's license) and bank accounts.[281] As a contrast to the Californian definition of personal information, state of South Carolina has narrowed down definition of personal information to only include data which can give access to a person's financial accounts or data that is possessed by a governmental or regulated entity.[282] The information issued by the governmental or regulated entity must uniquely identify an individual in order to count as personal information.[283] The state of South Carolina clearly makes definition of PII conditional - data has to give access to financial accounts; or data needs to be held by a government agency or regulated entity and must uniquely identify an individual.

If collected personal information is held by an unregulated private sector entity and such data uniquely identifies an individual, is the data still considered as PII or not? Due to state to state divergence and the definition of PII being dependent on sector-specific legal instruments or affected by lack of thereof, a straightforward answer to the question does not necessarily exists from the perspective of one state. If an indubitable general definition of PII does not exist *de jure* on a federal level, consumers in a highly codified state are axiomatically in a better position compared to those who live in a state that has not explicitly nor comprehensively included the definition of PII in any of the sector-specific legal instruments regulating data privacy. According to the data breach chart of 2016 published by Baker & Hostetler LLP only 34 states out of 50 have broader definition for personal information apart from the generally acknowledged term. Within the 34 state group the state of South Carolina is also included and its definition of personal information is rather vague and at face value conditional. Regarding collection of data, which is the first step taken in the process of BD exploitation, the definition of PII should be specific and given enough latitude in order to effectively address constant technological advancement taking place in the field of data science, especially in relation to utilization of BD at the commercial level. Most importantly, as the definition varies from state to state, there should be a federal instrument which would consolidate the definition of PII and therefore mitigate overall confusion revolving

[281] Baker & Hostetler LLP, Data Breach Charts, 2016, p.1-2.<https://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf>(5.4.2017)
[282] Id., p.7
[283] Id.

around the very definition. The commonly used term of PII, which only includes SSNs, numbers contained in various ID-cards, financial account information or credit card numbers[284] is a narrow spectrum in terms of PII revealed or produced via BD analytics. As it was mentioned in Chapter 4.1.2 that even innocuous data may cause concrete harm under specific circumstances. Although the FTC applies a definition of PII that more comprehensively takes into account multiple aspects underlying the literal meaning of personal data in the light of online behavioral advertising,[285] it should be stressed again that agency settlements are devoid of any precedential value. The Consumer Privacy Bill of Rights introduced back in 2012 under the Obama administration, which was never enacted, defined PII as follows:

"Any data, including aggregations of data, which is linkable to a specific individual. Personal data may include data that is linked to a specific computer or other device. For example, an identifier on a smartphone or family computer that is used to build a usage profile is personal data."[286]

The above definition managed to capture one of the most essential features applying to data analytics today; even an analysis of aggregated data may lead to a discovery of personal information falling under the definition of PII due to the fact that discovered data has potential to ameliorate consumer profiles linkable to specific individuals or devices.[287]

4.3.1 Finality principle and other grievances

The U.S data privacy regime has not adopted the "finality principle"[288] - PII should not be processed in ways incompatible with its initial collection purpose. Apart from the California Online Privacy Protection Act laying down specific notification requirements in relation to California residents, on a federal level privacy notices are only required mainly in relation to conduct falling within the scope of the earlier mentioned statutes:[289] GLB, COPPA, HIPAA and FCRA. In other words, if a conduct concerning data collection and processing falls outside the

[284] supra note 281
[285] Nancy J. King, Jay Forder, Data analytics and consumer profiling: Finding appropriate privacy principles for discovered data, Computer Law & Security Review: The International Journal of Technology Law and Practice (2016), p.9
[286] Id., p.8
[287] Id. p.9
[288] supra note 267, p.211
[289] Id., p.210

four federal statutes and state legislation is of no avail, there will be no obligation to inform about secondary use of collected PII. Considering the overall nature of BD analytics, purposes for which aggregated data is used may change drastically. Further, there is no general federal privacy policy, but the FTC in many instances has established that collecting PII without a consent is against the FTCA, such as the case concerning *VIZIO, INC. and VIZIO Inscape Services, LLC* mentioned in Chapter 4.2.2. Moreover, it is reasonable to presume that secondary use of data can be also held unfair or deceptive trade practice, if a company clearly deviates from its initial privacy notice.

The following can be regarded as other grievances in relation to data handling practices: (I) there are no general legal obligations to maintain internal records or to maintain any form of documentation with respect to PII possessed by data controllers; (II) there are no requirements to register any form of data processing activities; (III) there are no limits on cross-border data transfers; (IV) apart from the HIPAA, FCRA, COPPA and California's Shine the Light Law, there is no law of general application granting individuals access to their PII held by organizations; (V) there is no law of general application granting data subjects with other substantive rights, therefore the HIPAA and FCRA are only federal statutes providing some form of correction rights in relation to incorrect information; (VI) transfer of PII to companies that employ outsourced data processing services are not generally restricted apart from provisions contained in the HIPAA, GLB (except California and Massachusetts require organizations transferring PII to service providers to contractually maintain sufficient data protection safeguards).[290] Another grievance emanates from automated decision making. The FCRA is the only federal statute applying to pure private sector automated decision making, which only pays regard to employment decisions.[291]

5. Conclusion

What is a balance of rights between data controllers and data subjects in the context of BD employment for commercial purposes? A perfect balance could be described in a manner that takes comprehensively into account data subjects' rights attached to their provided data and guaranteeing maximum protection of PII whilst ensuring free flow of data within boundaries laid down by the sector-specific data privacy regime. From a federal perspective it is seemingly evident that a new legal instrument further consolidating the regime in relation to collection, storage and

[290] Id., p.212-213
[291] supra note 148, p.30

transfer of data, including an inclusive definition of PII with sensitive data categories, would be a much needed improvement in the current context. In terms of rendering consumer profiles via the utilization of BD, consumers should be able to correct incorrect PII with relative ease. Especially, under the FCRA, the process of informing a CRA first of incorrect information and hoping that the complaint also reaches the creditor is an unnecessary hurdle.[292] Moreover, if a consumer wants to rectify wrong information via a private right of action under the FCRA, the prerequisite of alleging a plausible claim works in favor of creditors and CRAs as consumers rarely possess any proof that communication regarding the incorrect information has been established between the creditor and CRA.[293] Although the FCRA classifies all persons who regularly collect information about consumers with the intention of selling or rendering consumer reports to third parties as CRAs, and is capable of capturing data brokers like in *United States V. Spokeo Inc. (2012)*, the above-stated conditional private right of action is a disadvantage from a consumer privacy perspective. It should be also noted that if a private sector entity well versed in BD exploitation does not fall under the definition "CRA", without proper state legislation in place, an aggrieved consumer will have slim chances to rectify incorrect information concerning him. Also the lack of general access rights to PII possessed by private companies with respect to data subjects is a significant factor undermining transparency in overall data processing in BD context.

Case *Spokeo, Inc., Petitioner v. Thomas Robins* (2016) well elucidated how an aggrieved data subject can litigate by resorting to the FCRA under circumstances revolving around incorrect PII.[294] In order to gain standing and instantiating a private right of action aimed to redress a wrong, plaintiffs have to establish that they have suffered *de facto* particular, concrete and actual harm. In other words, it is reasonable to presume that the damage suffered must be linkable to monetary and tangible loss in manner similar to *Federal Aviation Administration v. Cooper* (2012). Regardless, it should be acknowledged that data under specific circumstances can cause damage to data subjects, which is not necessarily measurable in actual money. For example, in *Spokeo, Inc., Petitioner v. Thomas Robins* wrongful information hindered only the plaintiff's employment opportunities. Other aspects in the aforesaid regard are also exacerbated due to lack of sensitive data categories on a federal level and courts unwillingness to recognize that even innocuous data bears the potential of causing concrete harm, if special attention is not paid to data quality nor the process of collection, storage and transfer.

[292] see Chapter 4.2.1
[293] see Chapter 4.2.1
[294] see Chapter 4.1.2

Regarding the FTCA enforced by the FTC, it is a poor example in the determination of rights between data subjects and data controllers due to agency settlements devoid of any precedential value caused by lack of private right of action.[295] If the FTC would be able to clearly delineate between unlawful and lawful conduct under the FTCA, courts would not be burdened by piggyback class action and the overall transparency concerning aspects of BD utilization could be significantly improved. It is also a major pitfall that past agency settlements are not enforceable and consumers cannot resort to filing for an injunctive relief.

In conclusion, taking into account other factors, such as state to state divergence being part of the U.S. sector-specific data privacy regime and other grievances mentioned in Chapter 4.3 & 4.3.1, it is likely that consumers in a nationwide context are not on an "equal footing" nor have sufficient rights in contrast to data controllers due to fundamental general rules missing from the federal regime. Reluctance to enact new federal instruments addressing apparent issues discussed within limits of the research has been justified on the basis of avoiding legal repercussions or by clinging to fear of causing an innovative standstill.[296] The U.S. congress refers this unwanted outcome as "unreasonable ossification".[297] It should be stressed that the very notion of rule of law is highly in discord with the above-stated justification. Even if BD contains massive commercial potential, it should not create an imbalance between the rights of data subjects and data controllers as it can negatively affect both parties, although the former party is to a great degree in a disadvantaged position in many aspects. Lastly, putting significant amount of faith in self-regulation and future legislative development taking place on a state level instead of improving the federal framework is not a guarantee of improved transparency in every state.

[295] see Chapter 4.2.2
[296] Lothar Determann; Adequacy of data protection in the USA: myths and facts. *International Data Privacy Law* 2016; 6 (3): 244-250, p.4
[297] Id.

List of References

Science books:

1. Frederick S. Lane, American Privacy: The 400-Year History of Our Most Contested Right, Beacon Press (November 1, 2009)

2. Einer Elhauge, The Fragmentation of U.S. Health Care: Causes and Solutions 1st Edition, Oxford University Press March 22, 2010

3. John K. Halvey, Barbara Murphy Melby, Business Process Outsourcing: Process, Strategies, and Contracts, 2nd Edition, John Wiley & Sons, Inc April 2007

4. Lyrissa Barnett Lidsky, R. George Wright, Freedom of the Press: A Reference Guide to the United States Constitution, Greenwood Publishing Group, 2004

5. Rosemary P Jay, Hunton & Williams, Lisa J Sotto and Aaron P Simpson, Getting the Deal Through - Data Protection & Privacy 2015, Law Business Research Ltd 2014

Science articles:

6. Kshetri, N. Big data's impact on privacy, security and consumer welfare, Telecommunications Policy (2014)

7. Clinton D. Lanier, Jr., Amit Saini, Understanding Consumer Privacy: A Review and Future Directions, Academy of Marketing Science Review volume 12, 1.1.2008

8. Max N. Helveston, Consumer Protection in the Age of Big Data, Washington University Law Review, Vol. 93, 2016

9. Alan Charles Raul, The Privacy, Data Protection and Cybersecurity Law Review - Edition 1, November 2014

11. Winston J. Maxwell, Principles-based regulation of personal data: the case of 'fair processing', International Data Privacy Law (2015) 5 (3): 205-216, 21 July 2015

12. Abu Bakar Munir, Siti Hajar Mohd Yasin, Firdaus Muhammad-Sukki, Big Data: Big Challenges to Privacy and Data Protection, World Academy of Science, Engineering and Technology International Journal of Social, Education, Economics and Management Engineering Vol:9, No:1, 2015

13. Ira S. Rubinstein, Big Data: The End of Privacy or a New Beginning?, International Data Privacy Law, 2013, Vol. 3, No. 2

14. Victoria D. Baranetsky, Social Media and the Internet: A Story of Privatization, 35 PaceL. Rev. 304 (2014)

15. Joel Reidenberg, The Data Surveillance State in Europe and the United States, 49 Wake Forest L. Rev. 583 (2014)

16. K. Krasnow Waterman, Paula J. Bruening; Big Data analytics: risks and responsibilities. International Data Privacy Law 2014; 4 (2): 89-95

17. Joanna Kulesza, International law challenges to location privacy protection, International Data Privacy Law, 2013, Vol. 3, No. 3

18. Fred H. Cate and Beth E. Cate, The Supreme Court and information privacy, International Data Privacy Law, 2012, Vol. 2, No. 4

19. Ohm, Paul, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization (August 13, 2009). UCLA Law Review, Vol. 57, p. 1701, 2010; U of Colorado Law Legal Studies Research Paper No. 9-12.

20. Solove, Daniel J., A Taxonomy of Privacy. University of Pennsylvania Law Review, Vol. 154, No. 3, p. 477, January 2006; GWU Law School Public Law Research Paper No. 129

21. Perri, Pierluigi and Thaw, David, Ancient Worries and Modern Fears: Different Roots and Common Effects of U.S. and EU Privacy Regulation (April 19, 2015). U. of Pittsburgh Legal Studies Research Paper No. 2016-06

22. Patrick L. Moore, United States v. Miller: Without a Right to Informational Privacy, Who Will Watch the Watchers, 10 J. Marshall J. Prac. & Proc. 629 (1977)

23. Pamela Samuelson, Privacy as Intellectual Property, 52 Stan. L. Rev.1125 (1999)

24. Mark Niles, Ninth Amendment Adjudication: An Alternative To Substantive Due Process Analysis of Personal Autonomy Rights, 48 UCLA L. REV. 85 (2000)

25. Erwin Chemerinsky, Rethinking State Action, 80 Northwestern University Law Review 503-557 (1985)

26. Lisa A. Kloppenberg, Avoiding Constitutional Questions, 35 B.C. L. Rev. 1106 (1994)

27. Clark D. Asay, Consumer Information Privacy and the Problem(s) of Third-Party Disclosures, 11 Nw.J. Tech.& Intell.Prop.321 (2013)

28. James T. O'Reilly, Deregulation and Private Causes of Action: Second Bites at the Apple, 28 Wm. & Mary L. Rev. 235 (1987)

29. Jeffrey Bils, 61 UCLA L. Rev. Disc. 226, Fighting Unfair Credit Reports: A Proposal to Give Consumers More Power to Enforce the Fair Credit Reporting Act (2013)

30. Rybnicek, Jan M. and Wright, Joshua D., Defining Section 5 of the FTC Act: The Failure of the Common Law Method and the Case for Formal Agency Guidelines (September 15, 2014). 21 (5) George Mason Law Review, 1287 (2014)

31. Stephanie L. Kroeze, The FTC Won't Let Me Be: The Need for a Private Right of Action Under Section 5 of the FTC Act, 50 Val. U. L. Rev. 227 (2015)

32. King, N. J. and Raja, V.T. (2013), What Do They Really Know About Me in the Cloud? A Comparative Law Perspective on Protecting Privacy and Security of Sensitive Consumer Data. Am Bus Law J, 50: 413–482

33. Nancy J. King, Jay Forder, Data analytics and consumer profiling: Finding appropriate privacy principles for discovered data, Computer Law & Security Review: The International Journal of Technology Law and Practice (2016)

34. Lothar Determann; Adequacy of data protection in the USA: myths and facts. International Data Privacy Law 2016; 6 (3): 244-250

35. 130 Harv. L. Rev. 437, Leading Case : 136 S. Ct. 1540 (2016), November 10, 2016.<http://harvardlawreview.org/2016/11/spokeo-inc-v-robins/>(25.2.2017)

36. 129 Harv. L. Rev. 1120, FTC v. Wyndham Worldwide Corp., February 10, 2016.<http://harvardlawreview.org/2016/02/ftc-v-wyndham-worldwide-corp/>(25.3.2017)

Case law:

37. Common Pleas Court of Cuyahoga County, No. 915,246., SHIBLEY v. TIME, INC., ET AL. (1974)

38. Appellate Court of Illinois, First District, First Division, No. 1-92-3944., Dwyer v. American Express Co. (1995)

39. U.S Supreme Court, 385 U.S. 374,Time, Inc. v. Hill. (1967)

40. U.S. Supreme Court, 389 U.S. 347, Katz v United States (1967)

41. U.S. Supreme Court, 425 U.S. 435, United States v Miller (1976)

42. U.S. Supreme Court, 416 U.S. 21, California Bankers Assn. v. Shultz (1974)

43. U.S. Supreme Court, 499 U.S. 340, Feist Publications v. Rural Telephone Service Co. (1991)

44. United States Court of Appeals, Ninth Circuit, 336 F.3d 811, KELLY v. ARRIBA SOFT CORP. (2003)

45. U.S. Supreme Court, 532 U.S. 67, FERGUSON et al. v. CITY OF CHARLESTON et al. (2001)

46. U.S. Supreme Court, 381 US 479, GRISWOLD V. CONNECTICUT (1965)

47. U.S. Supreme Court, 578 U. S. ____ (2016), Spokeo, Inc., Petitioner v. Thomas Robins (2016)

48. U.S Supreme Court, 547 U. S. ____ (2006), Kehoe v. Fidelity Federal Bank & Trust (2006)

49. United States District Court, Northern District of California, Case No: C 11-04674 SBA, Deacon v. Pandora Media, Inc. (2012)

50. United States District Court, Northern District of California, Case No: C 11-03764 LB, In Re: HULU Privacy Litigation (2012)

51. United States District Court, Northern District of California, Case No: C 11-cv-03764 LB, In Re: HULU Privacy Litigation (2015)

52. U.S. Supreme Court, 566 U. S. ____ (2012), Federal Aviation Administration v. Cooper (2012)

53. United States District Court for the Central District of California, Case No. 2-12-cv-05001-MMM-SH, United States v. Spokeo Inc. (2012)

54. FTC v. Wyndham Worldwide Corp

55. FTC, Attorney General of the State of New Jersey and Director of the New Jersey Division of Consumer Affairs v. VIZIO, INC. and VIZIO Inscape Services, LLC

56. FTC v. Snapchat Media, Inc.

57. FTC v. Sitesearch Corporation, dba LeapLab

Other sources:

58. 2016 TRUSTe/NCSA Consumer Privacy Infographic – US Edition, <www.truste.com/resources/privacyresearch/ncsa-consumer-privacy-index-us/>(05.01.2017).

59. Andrew Griffin, "Apple boss Tim Cook slams Google and Facebook for selling users' data", The Independent, Wednesday 3 June 2015. <http://www.independent.co.uk/life-style/gadgets-and-tech/news/apple-boss-tim-cookslams-google-and-facebook-for-selling-their-users-data-10295158.html>(13.1.2017).

60. Paul Rudo, "United States v. Miller: The 1976 Court Case That Determined Your Privacy Rights In The Cloud", EnterpriseFeatures, 25.08.2012.<http://www.enterprisefeatures.com/united-states-v-miller-the-1976-court-case-thatdetermined-your-privacy-rights-in-the-cloud/>(19.01.2017)

61. David N. Anthony, Alan D. Wingfield, Julie D. Hoffmeister and Virginia Bell Flynn, "Standing on Thin Air: Spokeo, Inc. v. Robins", Troutman Sanders LLP, 11.03.2015. <https://www.troutmansanders.com/standing-on-thin-air-spokeo-inc-v-robins-11-03-2015/>(29.1.2017)

62. Kiel Brennan-Marquez, "The Supreme Court's Big Data Problem", Data & Society: Points, 29.06.2016. <https://points.datasociety.net/the-supreme-courts-big-data-problem-9401fa88a3e0#.hllsyg5il>(7.2.2017)

63. Jeff John Roberts, "Supreme Court Rejects Privacy Claim in Data Broker Case", Fortune, 16.05.2016.<http://fortune.com/2016/05/16/supreme-court-spokeo-decision/>(7.2.2017)

64. Steve Orr, "Is your DMV data safeguarded properly?", Rochester (N.Y.) Democrat and Chronicle, 17.03.2015.<http://www.democratandchronicle.com/story/news/2015/03/16/dmv-data-security-sunshine-week-newyork-privacy/24846627/>(9.2.2017)

65. Allison Grande, "Hulu's Win Won't Halt Video Privacy Class Actions", Law360, April 1, 2015.<https://www.law360.com/articles/638399/hulu-s-win-won-t-halt-video-privacy-class-actions>(15.2.2017)

66. FTC Press Releases, "Spokeo to Pay $800,000 to Settle FTC Charges Company Allegedly Marketed Information to Employers and Recruiters in Violation of FCRA", June 12, 2012. <https://www.ftc.gov/news-events/press-releases/2012/06/spokeo-pay-800000-settle-ftc-charges-companyallegedly-marketed>(25.2.2017)

67. FTC Press Releases, "VIZIO to Pay $2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions without Users' Consent", February 6, 2017.<https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settlecharges-it>(25.3.2017)

68. FTC Press Releases, "Snapchat Settles FTC Charges That Promises of Disappearing Messages Were False", May 8,2014.<https://www.ftc.gov/news-events/press-releases/2014/05/snapchat-settles-ftc-charges-promisesdisappearing-messages-were>(26.3.2017)

69. FTC Press Releases, "Data Broker Defendants Settle FTC Charges They Sold Sensitive Personal Information to Scammers", February 18, 2016.<https://www.ftc.gov/news-events/press-releases/2016/02/data-broker-defendantssettle-ftc-charges-they-sold-sensitive>(27.3.2017)

70. AGATA DZIEDZIC | US Privacy Analyst, "California: "Common sense" encryption amendment incorporated into breach notification law", DataGuidance, 29 September 2016.<http://www.dataguidance.com/usa-californiaintroduces-common-sense-data-breach-notification-amendment/>(4.4.2017)

71. DLA Piper, Data Protection Laws of the World: United States.<https://www.dlapiperdataprotection.com/index.html?t=law&c=US>(4.4.2017)

72. Baker & Hostetler LLP, Data Breach Charts, 2016.<https://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf>(5.4.2017)

73. S. 668 — 114th Congress: Data Broker Accountability and Transparency Act of 2015." www.GovTrack.us. 2015. <https://www.govtrack.us/congress/bills/114/s668>(12.1.2017)

74. "H.R. 4516 — 114th Congress: Data Broker Accountability and Transparency Act of 2016." www.GovTrack.us. 2016. February 3, 2017 <https://www.govtrack.us/congress/bills/114/hr4516>(12.1.2017).

75. "H.R. 2977 — 114th Congress: Consumer Privacy Protection Act of 2015." www.GovTrack.us. 2015. February 3, 2017 <https://www.govtrack.us/congress/bills/114/hr2977>(13.1.2017).

76. U.S. Federal Trade Commissioner Julie Brill, Privacy and Data Security in the Age of Big Data and the Internet of Things, Delivered at Washington Governor Jay Inslee's Cyber Security and Privacy Summit January 5, 2016

77. CECILIA MUÑOZ, MEGAN SMITH, DJ PATIL, Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights, Executive Office of the President May 2016

78. Commissioner Julie Brill, "Big Data and Consumer Privacy: Identifying Challenges, Finding Solutions", Address at the Woodrow Wilson School of Public and International Affairs Princeton, University February 20, 2014

79. Marc Rotenberg, Alan Butler, T. John Tran, "Brief of Amici Curiae Electronic Privacy Information Center (EPIC) and Thirty Two Technical Experts and Legal Scholars in Support of Respondent", September 8, 2015

80. Hoofnagle, Chris Jay, New Challenges to Data Protection Study - Country Report: United States, January 20, 2010

81. Janet Cooper Alexander, An Introduction to Class Action Procedure in the United States, Presented Conference: Debates over Group Litigation in Comparative Perspective, Geneva, Switzerland, July 21-22, 2000

82. Federal Trade Commission Report, Big Data: A Tool for Inclusion or Exclusion?, January 2016

83. John E. Villafranco and Daniel S. Blynn, Kelley Drye & Warren LLP, "The Case of the Piggyback Class Action", September 2012

84. An ESET White Paper by Stephen Cobb, Data Privacy and data protection: US law and legislation, April 2016

85. Terence Craig, Mary E. Ludloff, Privacy and Big Data, O'Reilly Media, September 2011

86. Linda Koontz, CIPP/US, CIPP/G, Information Privacy in the Evolving Healthcare Environment, Health Management and Information Systems Soc, HIMMS 2013

87. Françoise Gilbert, Catherine D. Meyer, Denise Olrich, Paul T. Smith, Roy G. Weatherup, Privacy Compliance and Litigation in California: 2016 Update, CEB, September 2016

88. Daniel J. Solove & Chris Jay Hoofnagle, A MODEL REGIME OF PRIVACY PROTECTION Version 2.0, 05.04.2005