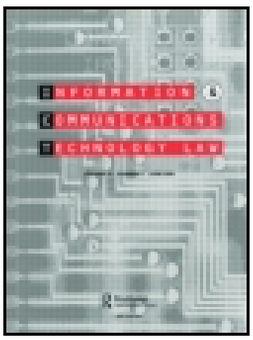

Routledge
Taylor & Francis Group

Information & Communications Technology Law

ISSN: 1360-0834 (Print) 1469-8404 (Online) Journal homepage: https://www.tandfonline.com/loi/cict20

A comparative analysis of the EU GDPR to the US's breach notifications

Chlotia Garrison & Clovia Hamilton

To cite this article: Chlotia Garrison & Clovia Hamilton (2019): A comparative analysis of the EU GDPR to the US's breach notifications, Information & Communications Technology Law, DOI: 10.1080/13600834.2019.1571473

To link to this article: https://doi.org/10.1080/13600834.2019.1571473

Published online: 25 Jan 2019.

INFORMATION & COMMUNICATIONS TECHNOLOGY LAW
https://doi.org/10.1080/13600834.2019.1571473

Routledge
Taylor & Francis Group

A comparative analysis of the EU GDPR to the US's breach notifications

Chlotia Garrison and Clovia Hamilton

Computer Science, Winthrop University, Rock Hill, SC, USA

ABSTRACT

One component of the newly implemented European Union General Data Protection Regulation (GDPR), a revision of a 1995 directive, is mandatory breach notification. The US has no such federal law. This means companies must satisfy multiple US laws and that makes it more challenging to comply. This study is a comparison of the GDPR with the statutes of the 50 US states, highlights the challenges companies face and reveals the types of decisions companies must make to be in compliance with these statutes.

KEYWORDS

Data breach; data breach laws; data protection laws; data protection; GDPR; privacy laws; personal data; identity crimes; identity theft; information security; notification of security breach; personal information; privacy

1. What is the GDPR?

In 2015, an agreement[1] was made between the European Parliament and the Council of the European Union[2] to develop the GDPR and implement it in May of 2018.[3] GDPR tightens the reigns on what companies can do with people's data by giving internet users more control over how their data is collected and used. The GDPR provides guidelines on what companies can and cannot do with their users' personal data. This personal data is any data that can identify a user including their name, demographics, phone number, IP address, online user name, sexual orientation, health data and political opinions. The guidelines stipulate that companies are to be more transparent and provide more clarity about the type of data they are collecting and using; and how the data will be used.[4]

Each company's user is to opt into the company's use of their personal data. In addition, companies are to use clear and simple language about how this is done along with

CONTACT Clovia Hamilton hamiltoncl@winthrop.edu

[1]Ari Shapiro, *What The European Union's New Online Privacy Law Means For The U.S.* (2018) See also, Tal Z Zarsky, 'Incompatible: The GDPR in the Age of Big Data' (2016) 47 SHLR 995. Zarsky explains how the GDPR replaces the 1995 Data Protection Directive (DPD) formally known as the Council Directive 95/46/EC of the European Parliament and of the Council of 24's October 1995 directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 OJL 282/32.

[2]David Greene, *Sweeping Internet Privacy Protectioni Regulations to Take Effect* (National Public Radio 2018).

[3]Jan Philipp Albrecht, 'How the GDPR Will Change the World' (2016) 2 EDPLR 287.

[4]Parminder Bahra, Mark Kelly, George Downs, Monika Piszczek, and Andy Pirlogea, 'The European Union's General Data Protection Regulation on Data Privacy Will Come Into Force on May 25, 2018' (*Wall Street Journal (WSJ)*, 2018) <www.wsj.com/video/gdpr-what-is-it-and-how-might-it-affect-you/2A0C50F6-6248-49EE-AAFC-A505CB425705.html> accessed 24 December 2018. See also the EU GDPR, *EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1* (European Union 2016); 2016 OJ (L119/33), Ch 1, Art 4(1).

required privacy notices.[5] Non-compliance with the GDPR will result in a significant punitive penalty equal to the larger of 20 Million Euros which is $24 Million USD; or 4% of the annual turnover.[6]

2. Why was the GDPR introduced?

2.1. Increasing data breaches and lack of enforcement

Article 8 of the Charter of Fundamental Rights of the European Union gives citizens of the EU the right to protection of their personal data.[7] Prior to the enactment of the GDPR, the EU was operating under a 1995 Directive. The GDPR follows the EU's 1995 Data Protection Directive 95/46/EC which required member states to protect the processing and free movement of personal data.[8] However, there have been an increasing number of data breaches and a lack of enforcement.[9] Directives are not legally binding and serve to achieve a particular result without dictating the means of achieving that result.[10] Directives normally leave member states with a certain amount of freedom as to the exact rules to be adopted. The member states must transpose the directive into internal law. Directive 95/46/EC on the protection of personal data had to be transposed by the end of 1998. This was accomplished with the 1998 Data Protection Act.[11] Since all member states have enacted their own data protection legislation, there was a need for unification of these laws.

In addition, since the old European data protection Directive was written before entering into the Fourth Industrial Revolution (4IR) of using smart phones, smart homes, smart cars and smart workplaces; and before massive amounts of big, sensitive information was collected, there was a need for an updated, more modern law.[12] In 2016, the 4IR was first coined by Klaus Schwab, the executive chairman of the World Economic Forum. He later wrote a book entitled *The Fourth Industrial Revolution* that describes how this fourth revolution is fundamentally different from the previous three, which were characterized mainly by advances in technology. The underlying basis for 4IR lies in advances in communication and connectivity rather than technology.[13]

Further, increasingly consumers are expecting more transparency about the collection of their data.[14] Also note that data breaches and lack of enforcement is also a

[5]GDPR (n 4). See also, Ailsa Chang, *Europe's New Online Privacy Rules Could Protect U.S. Users Too* (National Public Radio 2018). In addition, see Lulu Garcia-Navarro, *European Data Privacy Rules to Go into Effect* (2018).
[6]Bahra (n 4).
[7]EU Charter of Fundamental Rights, *EU Charter of Fundamental Rights of the European Union: Regulation (EU) 2012/326 of the European Parliament and of the Council of 18 December 2000 to Strengthen the Protection of Fundamental Rights in the Light of Changes in Society, Social Progress and Scientific and Technological Developments by Making Those Rights More Visible in a Charter. OJ 2012 C 326/1* (European Union 2012).
[8]EU Directive 95/46, *EU Directive 95/46: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (1995); Zarsky (n 1).
[9]Shapiro (n 1). See also, Sebastian J Golla, 'Is Data Protection Law Growing Teeth: The Current Lack of Sanctions in Data Protection Law and Administrative Fines under the GDPR' (2017) 8 JIPITECL.
[10]Sybe de Vries, Ulf Bernitz and Stephen Weatherill, *The EU Charter of Fundamental Rights as a Binding Instrument: Five Years Old and Growing* (Bloomsbury 2015).
[11]Data Protection Act, *Data Protection Act 1998, Chapter 29* (The Stationery Office (TSO) 1998).
[12]Bahra (n 4). See also, David Greene, *Why a Europe-Wide Data Protection Law Matters to Others* (2018).
[13]Klaus Schwab, *The Fourth Industrial Revolution What It Means and How to Respond* (Council on Foreign Relations 2015).
[14]Chang (n 5). See also Stacy-Ann Elvy, 'Paying for Privacy and the Personal Data Economy' (2017) 117 CLR 1369.

problem for EU citizens given the difficulty of enforcing privacy laws in foreign jurisdictions.[15]

2.2. Unification of data protection laws

In addition, the GDPR was introduced to provide a unified data protection law for the EU to replace all of the existing Member State' provisions.[16] There are 28 Member States in the EU including Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK.[17] The UK confirmed their exit from the EU (called 'Brexit') by vote in June 2016. It was anticipated that UK's break from the EU would involve lengthy negotiations which would take years.[18] However, the regulation is already in force and the UK has said that it will continue to follow the standards set by the GDPR. The Queen's Speech on 21 June 2017 confirmed that after its departure from membership of the EU, the Government's intention is to bring the GDPR into UK law to ensure that UK's data protection framework is 'suitable for our new digital age, allowing citizens to better control their data'.[19] For example, a new UK Data Protection Act (DPA) was passed just before the GDPR became effective. According to Elizabeth Denham, the UK's Information Commissioner in charge of data protection enforcement, the GDPR should only be a 'step change' for companies that were already complying with the UK DPA.[20]

The goal of the GDPR was to bring more legal certainty and coherence between the 28-member states' legal systems. Some critics have argued that the GDPR will create more national differences because the enactment of this regulation was a shift from a directive to a regulation. Yet, the 28 Member States still have competencies and control over their media and press laws, national security and their defense.[21]

3. GDPR implementation challenges for companies

The GDPR has and will have a significant effect on companies outside of the EU, including the US, because these businesses collect or use EU residents' data. In addition, many companies outside of the EU use companies based in the EU for services and for processing data.[22] Although only 11% of the 150 International Association of Privacy Professionals (IPAA)'s survey disclosure statements mention the GDPR as a compliance risk,[23] the GDPR takes a risk-based approach to data protection. There are heightened requirements such as consultations with data protection authorities for companies that engage in high

[15]Mira Burri and Rahel Schär, 'The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-driven Economy' (2016) 6 JIP 479.
[16]Albrecht (n 3).
[17]European Union, 'Countries' (*European Union*, 2018) <https://europa.eu/european-union/about-eu/countries_en> accessed 1 August.
[18]Melissa Hendrie, 'Brexit: Is This the End for the General Data Protection Regulation?' (2016) 37 BLR 173.
[19]Queen Elizabeth Queen Elizabeth II, *The Queen's Speech and Associated Background Briefing, on the Occasion of the Opening of parliament* (2017).
[20]Matt Burgess, *What is GDPR? The Summary Guide to GDPR Compliance in the UK* (Conde Nast 2018).
[21]Albrecht (n 3).
[22]Bahra (n 4).
[23]IPAA, *Privacy Risk Study 2017: PII Remains top Information Risk* (2017).

risk activities. High risk activities include automated profiling, large-scale processing of data, and other activities that will result in a high risk to individual rights and freedoms. The other categories are at-risk and low risk activities.[24]

Automated profiling is any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.[25] The GDPR does not provide a definition for large scale data processing. Yet, some member states have provided GDPR guidelines. For example, the UK's Information Commissioner's GDPR guidelines provides that the GDPR does not contain a definition of large-scale processing, but to decide whether processing is on a large scale you should consider: (1) the number of individuals concerned; (2) the volume of data; (3) the variety of data; (4) the duration of the processing; and (5) the geographical extent of the processing.[26] They note that examples of large-scale processing include a hospital (but not an individual doctor) processing patient data; tracking individuals using a city's public transport system; a fast food chain tracking real-time location of its customers; an insurance company or bank processing customer data; a search engine processing data for behavioral advertising; or a telephone or internet service provider processing user data. Further, they note that when individual professionals process patient or client data, they are not processing on a large scale.[27]

3.1. The right to be forgotten

EU residents have the right to be forgotten under the GDPR. Some EU member state legislators, such as the Slovak legislation, enacted this right in 2014. The Court of Justice of the European Union (CJEU) confirmed this right in its judgment in the 2014 *Google Spain, Google Inc.* vs. *Agencia Esapanola de Preoteccion de Datas (AEPD), Mario Costeja Gonzalez* case.[28] That is, they have the right to request to have their data be deleted.[29] With regard to data storage, personal data needs to be encrypted and managed in a manner that allows it to be categorized using data mapping for future retrieval and periodic reviews.[30] Companies also need to make sure that users' data can be transferred using a common file type. This is called the right to data portability.[31] Thus, if a user wants to

[24]Gabriel Maldoff, *The Risk-based Approach in the GDPR: Interpretation and Implications* (2016). See also Natalia Daśko, 'General Data Protection Regulation (GDPR)–Revolution Coming to European Data Protection Laws in 2018. What's New for Ordinary Citizens?' (2018) 23 CLR 123. Dasko discusses privacy risk assessments and how the notion of privacy by design and privacy by default were adopted at the 32nd International Conference of Data Protection and Privacy Commissioners in 2010. The GDPR makes this a legal obligation. See GDPR (n 4) at 2016 OJ (L119/33) §4 Art (4); and Preamble Recitals 84, 94–96.

[25]GDPR (n 4);UK Information Commissioner's Office (ICO) GDPR Guide, *What is Automated Individual Decision-making and Profiling?* (2018).

[26]GDPR (n 4) at 2016 OJ (L119/53) Chap IV §3 Art (35); and Preamble Recital 81.

[27]UK ICO GDPR Guide (n 25).

[28]Zuzana Lenzová, and Byung Park, 'Slovak Republic: Data Protection Reform' (2017) IFLR 17. See also Joy Liddicoat, 'Right to Be Forgotten' (IT and Online Law Conferences). Google v. Spain, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, E.C.J. C Court of Justice of the European Union, 131/12* (2014).

[29]Bahra (n 4).

[30]Olly Jackson, 'EMEA: One Problem After Another' (2018) IFLR. See also, David Flint, 'Reaching Out for DP Compliance' (2017) 38 BLR 206; also regarding encryption, see GDPR (n 4) at 2016 OJ (L119/51) § 2Art 32(1)(a); 2016 OJ (L119/36) §2Art 6(4)(e); and Preamble Recitals 60, 83.

[31]Garcia-Navarro (n 5). See also, Albrecht (n 3).

switch from using Facebook to some other social media platform, they should be able to easily get a copy of their data and transfer it.

However, the right to be forgotten is not an absolute right as certain conditions apply.[32] Under the GDPR, the data is to be erased without undue delay if one of six grounds applies: (1) the personal data is no longer necessary in relation to the purposes for which it was collected or processed; (2) the data subject withdraws consent; (3) the data subject objects to the processing; (4) the personal data have been unlawfully processed; (5) the personal data needs to be erased for compliance with a legal obligation; or (6) the personal data has been collected in relation to an offer of information society services. Further, the grounds do not apply if data processing is necessary for the exercise of freedom of expression and information; compliance with a legal obligation; a health-related public interest reason; to establish, exercise or defend a legal claim; or for a public interest related archival purpose.[33]

Nevertheless, the right to be forgotten can hurt small, medium and large sized businesses that rely on the business model of selling the collected personal data to advertisers and other third parties seeking that information. In particular, Facebook is under close observation and scrutiny. Although large internet-based companies such as Facebook were not founded in Europe, the GDPR impacts their capture and use of European residents' personal data.

It has also been advocated that social media marketing intermediaries such as Facebook should be held accountable to assist users in developing an understanding of digital citizenship and pay more attention to the dignity and safety of their users. Although, they handle a number of cyber bullying, harassment and other abuse complaints, the decisions Facebook makes are vague and indecisive.[34] There seems to be a lack of transparency. In 2018, Facebook was in the news when Facebook's founder, Mark Zuckerberg, was asked to answer to the US Congress regarding their user privacy practices and transparency issues.[35] Facebook lost control over data for 87 million users in a recent scandal. The scandal involved the improper harvesting of Facebook user data by the political consulting firm Cambridge Analytica.[36] Some critics of the GDPR have stated that it is, for political reasons, deliberately ambiguous, confusing and difficult to implement so that it can be interpreted in favor of political actors or in favor of internet-based companies like Facebook.[37] Facebook's CEO, Mark Zuckerberg, has been criticized for leaning toward a minimalist interpretation of the GDPR; for stating that Facebook will apply the GDPR 'in spirit'; and for moving in the direction of applying only some of the GDPR protections worldwide.[38]

[32]Bahra (n 4).
[33]GDPR (n 4) at 2016 OJ (L119/43) §3, Art 17, Right to Erasure and Preamble Recital 66.
[34]Danielle Citron and Helen Norton, 'Intermediaries and Hate Speech: Fostering Digital Citizenship for Our Information Age' (2011) 91 BULR 1435.
[35]Matt Carlson, 'Facebook in the News: Social Media, Journalism, and Public Responsibility Following the 2016 Trending Topics Controversy' (2018) 6 DJ 4. See also, Tony Romm, 'Facebook's Zuckerberg Just Survived 10 Hours of Questioning by Congress' *Washington Post* (Washington, DC) <www.washingtonpost.com/news/the-switch/wp/2018/04/11/zuckerberg-facebook-hearing-congress-house-testimony/?noredirect=on&utm_term=.8eacc4864efd> accessed 20 June 2018.
[36]Chang (n 5). See also, Garcia-Navarro (n 5).
[37]Henry Farrell and Abraham Newman, 'Here's How Europe's Data Privacy Law Could Take Down Facebook' *Washington Post* (Washington, DC) <www.washingtonpost.com/news/monkey-cage/wp/2018/05/25/heres-how-europes-gdpr-may-take-down-facebook/> accessed 31 July 2018.
[38]Garcia-Navarro (n 5); Farrell and Newman (n 37); and see Aarti Shahani, *3 Things You Should Know About Europe' Sweeping New Data Privacy Law* (National Public Radio 2018).

3.2. Lengthy GDPR provisions

Another problem with the GDPR is its length.[39] The GDPR contains 173 preamble items in addition to 99 articles across 11 chapters. The directive that was replaced contained 72 preamble items and 32 articles across 7 chapters and 3 additional articles in the final provisions. Other countries developing a unified law similar to the GDPR should seek more concise provisions.

3.3. Privacy notices

Just prior to the GDPR going into effect, consumers began to see and receive new privacy notices. Companies began to update their terms of service and data security rules. Companies are required to explain the privacy laws in simple language and they are required to provide easy to follow prompts.[40] Yet, critics complain that companies' online policies are now much longer. The companies are required to state what data is being collected; how and why they are using the data; and provisions for giving the user the ability to control what the company does with the data. Companies are required to use fewer pre-ticked, pre-selected boxes.[41] Some companies began to work on updating their policies once the GDPR was passed, and others are now scrambling to comply.

4. Possibilities for a US federal statute similar to the GDPR

The driver of data protection reform in the EU and the motivation behind the GDPR has much to do with 'deep cultural values and understandings' about privacy rights in the EU which were expressed in the 1995 Directive and the aforementioned *Charter of Fundamental Rights of the European Union* which covers broader societal contexts.[42] Thus, in the EU, there is grave concern about individual privacy that translates into duty to protect individual data. Further, the EU is critical of countries that do not protect data to their standard.[43] This is spreading because some countries such as Japan, Brazil and South Korea are currently discussing introducing provisions similar to the GDPR.[44] Why not the US?

The safe harbor agreement between the EU and US was to provide the principles for protection of EU citizens' personal data in US business undertakings.[45] Yet, there are

[39]Albrecht (n 3).

[40]Chang (n 5). See also, Mary Louise Kelly, *How Europe's New Data Privacy Law Is Supposed To Give Users More Control* (National Public Radio 2018).

[41]Bahra (n 4). See GDPR (n 4) at 2016 OJ (L119/48) Chap IV§1 Arts 25–26. With regard to pre-ticked boxes, see Preamble Recital 32.

[42]Burri and Schär (n 15). See also David Flint, 'Can of Worms?' (2018) 39 BLR 54 Flint urges a broader reflection on the paradigm shift in behavior regarding the use of data in a data driven economy beyond the current focus on tech-savvy businesses. This notion is also mentioned in Elvy (n 14). See also EU Charter Fundamental Rights Analyzed, *Charter of the Fundamental Rights of the EU Right by Right Analysis* (2017); EU Charter of Fundamental Rights, *EU Charter of Fundamental Rights of the European Union: Regulation (EU) 2012/326 of the European Parliament and of the Council of 18 December 2000 to Strengthen the Protection of Fundamental Rights in the Light of Changes in Society, Social Progress and Scientific and Technological Developments by Making Those Rights More Visible in a Charter. OJ 2012 C 326/1*.

[43]Hendrie (n 18).

[44]Albrecht (n 3). See also, Adam Satariano, 'G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog' *The New York Times* (NYC, NY) <www.nytimes.com/2018/05/24/technology/europe-gdpr-privacy.html> accessed 31 July 2018.

[45]Farrell and Newman (n 37). See also Paul M Schwartz, 'The EU-US Privacy Collision: A Turn to Institutions and Procedures' (2012) 126 HLR 1966. See also Hendrie (n 18); and Flint (n 30).

different understandings of privacy and the regulation of privacy in the EU and the US which has resulted in much political wrangling.

4.1. Data breach notification attempts

In the US, the first federal data breach notification bill was introduced in Congress in 2003. Though read twice, it never exited the Judiciary Committee.[46] In 2015, the sitting president of the US proposed the Personal Data Notification & Protection Act (PDNPA). The PDNPA of 2015 introduced in Congress provided federal notification guidelines for businesses that handle the personal information of more than 10,000 individuals in a 12-month period. Though it was referred to multiple committees, it had a similar fate to all proposed federal data breach notification laws to date. It never came out of committee.[47] In 2007 alone three data breach laws were introduced in Congress without success.[48]

4.2. Absolute right to be forgotten

The US state laws do not contain the right to be forgotten. If the US makes the right to be forgotten absolute, will it be fair to companies like Facebook? Note that Facebook provides its user platform for free. The free wielding removal of all user data would crush Facebook's business model and could cause internet-based companies like Facebook to go out of business. This also begs the question, 'how best to weigh a technology giants' ability to monetize consumers' personal data against the rights of the individual consumers to their personal data?'. It has been noted that some countries do not have security breach laws requiring notices to individual citizens. Instead, for example, their laws might only pertain to data handled by government agencies and only require notification to government agencies.[49] In these instances, it seems that the individual's right to privacy is not being recognized. As aforementioned, in the EU, the *Charter of Fundamental Rights of the EU* imparts everyone with the right to protection of personal data. The Charter's Article 8 covers Protection of personal data and is set forth in Title II Freedoms. It states that:

- 'Everyone has the right to the protection of personal data concerning him or her;
- Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law; and
- Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified'.[50]

[46]Rachel German, 'What Are the Chances for a Federal Breach Notification Law?' Identity Experts Blog <https://identity.utexas.edu/id-experts-blog/what-are-the-chances-for-a-federal-breach-notification-law> accessed 25 August 2018. See also, S. 1350 – 108th Congress: Notification of Risk to Personal Data Act (www.Congress.gov. 2003) <www.Congress.gov/bill/108th-congress/senate-bill/1350/all-actions?q=%7B%22search%22%3A%5B%22S.+1350+%5Cu2014+108th+Congress%3A+Notification+of+Risk+to+Personal+Data+Act%22%5D%7D&r=2&overview=closed#tabs> accessed 25 August 2018.

[47]HR. 1704 – 114th Congress: Notification of Risk to Personal Data Act (www.Congress.gov. 2003) www.congress.gov/bill/114th-congress/house-bill/1704/all-actions?overview=closed#tabs accessed 25 August 2018.

[48]Consumer Privacy Protection Act, *Consumer Privacy Protection Act* (2017). See also the PDNPA, *Personal Data Notification and Protection Act (PDNPA)* (2017).

[49]David Banisar, *The Right to Information and Privacy: Balancing Rights and Managing Conflicts* (Access to Information Program 2011).

[50]Personal Data Notification and Protection Act (n 48).

The US has a *Bill of Rights* set forth in the first 10 amendments to the US Constitution. With respect to property rights, Amendment 5 is called the Due Process Clause and states that a US citizen shall not be deprived of property without due process of the law and private property shall not be taken for public use without just compensation.[51] There is no amendment to the US Constitution focused on personal data. Amendment 5 is typically associated with tangible property or intellectual property and not personal data. In general, it is unlikely that Americans think of their personal data as property to be compensated for and not deprived of. Perhaps this is why US technology companies have been able to monetize the use of personal data.

To thwart fears about the potential misuse of internet users' personal data, a bill called the California Consumer Privacy Act of 2018 recently passed in the State of California. The law, passed by the legislature, includes a provision that consumers can request deletion of any personal information,[52] and businesses must provide information about how a consumer's personal information was sold or disclosed. This initiative met with opposition from technology companies such as Facebook, Google and Netflix as represented by the Internet Association. The opposition is rooted in the fact that these companies see this legislation as a threat to their business models.[53] In fact, Safari anticipated an influx of online users who would exercise their right to be forgotten once the GDPR was enacted in May of 2018.[54] It is estimated that Facebook loss three million users in Europe due to the GDPR.[55] Given the opposition from technology companies and the loss of users that Facebook experienced, it is not hopeful that the US will adopt a unified body of law such as the GDPR. However, Zarsky points out that the EU's optimism toward the changes that the GDPR brings about will impact global firms operating in the US and American consumers. Given that the American firms must make costly changes, they might 'opt for complying with one regulatory model everywhere'.[56]

4.3. Impediments to a similar federal law

A major obstacle to a federal US law is states' rights. A federal law would preempt state law. A federal notification law might be less restrictive than existing state law reducing the protections of that state's citizens. Likewise, it might be more restrictive, expanding the scope of current state law.[57] In addition, the GDPR differs from the US privacy model.[58] The GDPR has a broader definition of personal data as used in the definition of data breach. The EU definition includes any data that can be directly or indirectly

[51] US Bill of Rights, *US Constitution Annotated: Amendments, Articles in Addition to, and Amendment of, the Constitution of the United States of America, Proposed by Congress, and Ratified by the Several States, Pursuant to the Fifth Article of the Original Constitution* (1791).
[52] Art Neill, *What You Should Know About the New California Consumer Privacy Law* (Forbes, Inc. 2018).
[53] Mary Louise Kelly, *Do Not Sell My Personal Information: California Eyes Data Privacy Measure* (National Public Radio 2018).
[54] Beata Safari, 'Intangible Privacy Rights: How Europe's GDPR Will Set a New Global Standard for Personal Data Protection' (2016) 47 SHLR 809.
[55] Elizabeth Dwoskin and Hayley Tsukayama, 'Facebook Shares Tank on Slowing Growth, Wiping Out Billions in Value' *Washington Post* (Washington, DC 25 July) The Switch <www.washingtonpost.com/technology/2018/07/25/facebook-shares-fall-percent-revenue-miss/?noredirect=on&utm_term=.706c86ed0a06> accessed 4 August 2018.
[56] Zarsky (n 1).
[57] German (n 46).
[58] Jay Cline, 'Data Breach Notification: 10 Ways GDPR Differs from the US Privacy Model' Broader Perspectives <www.pwc.com/us/en/services/consulting/cybersecurity/library/broader-perspectives/gdpr-differences.html> accessed 25 August 2018.

associated with a living individual.[59] Individual identifiers can be as simple as a name, a number, an IP address, a cookie identifier, or other factors. If it is possible to identify an individual directly from the information you are processing, then that information may be personal data. However, there may be instances when all identifiers have been removed and a person may be identified indirectly by combining data. In this instance, there is a need to take into account the information that is being processed together with all the means reasonably likely to be used, by either the processor or any other person, to identify an individual. This is important to thwart inadvertent releases or disclosures of information that could be linked with other information and inappropriately identify an individual.[60]

Exemplar types of information that could allow an individual to be indirectly identified include car registration numbers, Vehicle Identification Numbers (VINs); national insurance numbers; combinations of 'significant criteria' such as age, occupation and residence address; or passport numbers. The key is that these types of information can be linked to other information and can result in the identification of the individual. For example, '[a] vehicle's registration number can be linked to other information held about the registration (e.g. by the Driver & Vehicle Licensing Agency to indirectly identify the owner of that vehicle)'.

The UK ICO provides the example where an individual submits an application for a job. Upon receiving the application, the organization's HR department removes the first page, which contains the individual's name, contact details, etc. and saves the remainder of the form in 'Folder 1'. The application form is saved with a randomly generated application number and sent on to the recruiting manager. In a restricted-access folder, 'Folder 2', the HR department stores the first page of the application, alongside the application number. The information in Folder 1 does not allow for the identification of any individual. However, when it is combined with the information in Folder 2, the applicant can be identified.

Sometimes, whether someone can be identified may depend on who may have access to the information and any other information that can be combined with it. It's important to be aware that you may hold information, which when combined with other information held outside of your organization, could lead to an individual being indirectly identified or identifiable.

The UK ICO provides two examples. First, an online platform releases statistical data sets about the use of its services for research purposes. This information does not contain the names of the services users, but instead profile data showing usage patterns. However, a number of those individuals have made public comments about their use of the platform. The information released by the platform can be matched to the public comments to identify those individuals. Second, a public authority releases information about complaints in response to a request under Freedom of Information Act 2000. It does not reveal the names or addresses of the complainants, but other information is in the public domain that can easily be used to match the identity of those complainants.

[59]GDPR (n 4) at 2016 OJ (L119/33) Chap I Art 4(1); (L119/32) Chap I Art (2); (L119/38) Chap II Art (9); (L119/39) Chap II Art (10); and Preamble Recitals 1–2, 26, 57.

[60]UK Information Commissioner's Office (ICO) GDPR Guide, *Can We Identify an Individual Indirectly From the Information We Have (Together With Other Available Information)?* (2018).

The US model focuses on sensitive personal information such as social security numbers and elements that allow access to financial information. The GDPR does not require a company to report a breach if the company has in place 'appropriate technical and organizational measures' such as pseudonymization and encryption The organizational measures include an organization's ability:

- to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- to have a process for regularly testing, assessing an and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.[61]

In the US model, the data itself must be encrypted. Also, the GDPR requires companies to document the facts of the data breach and the remedial action taken to prevent a reoccurrence. This is an uncommon requirement in the US laws.

5. GDPR and US data breach notification laws

5.1. Notices to supervisory authorities of data breaches

The GDPR requires data controllers to inform the supervisory authority of a data breach without undue delay and where feasible within 72 hours of becoming aware of the breach. If the notification is not done within 72 hours, the controller must provide an explanation of the delay with the notification.[62] The notification is at the member state level. The US statutes vary widely in regard to notifying an authority. Most states require notification only if the breach might lead to identity theft or other harm to the individual.[63] A few states require companies to notify the state Attorney General for every breach. Some states require the data controller to notify the state attorney general if 500 or, most prevalent, 1000 consumers are impacted. Others require the data controller to notify the Consumer Reporting Agencies if 500 or 1000 consumers are impacted. Some data breach notification laws only require notifying the impacted individuals.[64]

5.2. Notices to consumers of data breaches

The GDPR requires the controller to notify the data subjects 'without undue delay'.[65] According to the National Conference of State Legislatures (NCSL), legislation has been enacted by all 50 states, the District of Columbia, Puerto Rico and the US Virgin Islands that requires private entities or government agencies to notify individuals who have

[61]GDPR (n 4) at 2016 OJ (L119/51) Chap IV § 2 Art 32(1); and (L119/33) Chap I Art 4(5) definition of pseudonymization.
[62]GDPR (n 4) at 2016 OJ (L119/52) Chap IV §2Art 33(1). See also, IFLR, 'European In-House Summit: Key Takeaways' (2017) IFLR 53. A International Financial Law Review (IFLR) Fifth In-House Summit. The Summit takeaway is for companies to be prepared with instant response plans. In addition, see Paul M Schwartz, 'Information Privacy in the Cloud' (2012) 161 UPLR 1623.
[63]Elizabeth Snell, 'Attorneys General Stress Need for State Data Breach Laws' Health IT Security.
[64]Baker Hostetler, *Baker Hostetler Data Breach Charts*, 2018.
[65]GDPR (n 4) at Preamble Recital 86.

been impacted by security breaches.[66] There are 50 states and the last two to adopt such laws were South Dakota and Alabama. Similar to the GDPR, most US states require notification without unreasonable delay. However, in the US, 18 states include a specific deadline for notifying affected individuals; 2 require a 30-day notice, 2 states require a 60-day notice, 1 has a 90-day limit; 1 has a 15 day notice for medical information; 1 requires notice 7 business days after law enforcement review; and the remaining 11 states require a 45-day notice.[67]

Further, the GDPR and all US state statutes allow a delay for law enforcement or to secure the system from further exposure.[68] As per Preamble Recitals 85–88 of the GDPR, a notifiable breach must be reported to the relevant supervisory authority without undue delay and within 72 hours of discovery. The GDPR recognizes that it will often be impossible to investigate a breach fully within that time-period and allows notification to provide information in phases. If all the information cannot be provided within 72 hours, the reasons for the delay must be provided in the breach notification. If a breach is sufficiently serious to warrant notification to the public, you must do so without undue delay.[69]

In the US, Maine provides that notification may be delayed for no longer than 7 business days after a law enforcement agency determines that the notification will not compromise a criminal investigation.[70] Maryland's and South Dakota laws state that notification is required not later than 30 days after law enforcement determines it will not impede a criminal investigation. The other states allow a delay if notification would impede a criminal investigation.[71]

Further, delays have been allowed to investigate intrusions. For example, in 2014, hackers stole credit and debit card information from 70 million Target store customers and there was a delay in the notices to Target's customers of four days after they confirmed that there was breach.[72]

5.3. Contents of data breach notifications

The GDPR notification 'should' include a description of the data breach and recommendations on mitigating the potential damage.[73] Some US statutes state only that the notification must be made without any guidelines on the contents of the notification. Several

[66]NCSL, 'Security Breach Notification Laws' (*National Conference of State Legislators (NCSL)*, 2018) <www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx> accessed 13 December.

[67]The State of Colorado and Florida have a 30-day notice requirement; Delaware and South Dakota have the 60-day notice requirement; Connecticut requires a 90-day notice; and the states that require a 45-day notice includes: Alabama, Arizona, Maryland, New Mexico, Ohio, Oregon, Rhode Island, Tennessee, Vermont, Washington and Wisconsin. Maine requires 7-day notice after a law enforcement agency makes a determination (rather than from the discovery date); and California has a 15-day notice requirement for medical information. The respective statutes are: Colorado Statute, *Colo. Rev. Stat. § 6-1-716 Title 6 Consumer and Commercial Affairs, Notification of Security Breach* (2016); Delaware Statute, *Del. Code Tit. 6, § 12B-101 et seq., Title 6 Commercial and Trade, Subtitle II Other Laws Relating to Commerce and Trade, Chapter 12B. Computer Security Breaches* (2018).

[68]GDPR (n 4) at Preamble Recitals 86 and 88.

[69]GDPR (n 4) at Preamble Recitals 85–88; UK Information Commissioner's Office (ICO) Data Protection Act Law Enforcement Guide, *Guide to Law Enforcement Processing (Part 3 of the DP Act 2018)* (2018).

[70]Maine Statute, *Me. Rev. Stat. Tit. 10 § 1346 et seq., Notice of Risk to Personal Data Act, Security Breach Notice Requirements* (2005).

[71]Baker Hostetler (n 64);Maryland Statute, *MD COMM L Code § 14-3504 Commercial Law Title 14 – Miscellaneous Consumer Protection Provisions Subtitle 35 – Maryland Personal Information Protection Act – Security breach* (2015); and South Dakota Statute, *S.D. Cod. Laws §§ 22-40-20 to -46, Chapter 22-40 Identity Crimes* (2018).

[72]Karen Freifeld, 'U.S. Companies Allowed to Delay Disclosure of Data Breaches' <www.reuters.com/article/us-target-data-notification/u-s-companies-allowed-to-delay-disclosure-of-data-breaches-idUSBREA0F1LO20140116> accessed 25 August 2018.

[73]GDPR (n 4) at Preamble Recital 86.

US states provide guidance on what information to include in the notifications of breaches (i.e. the 'content' of the notification).[74] Features included by the states that provide guidelines are: the approximate date of the breach; a description of the personal information included in the breach; actions taken to restore the security and confidentiality of the information involved in the breach; steps a consumer can take to protect himself or herself from identity theft; toll-free telephone numbers and addresses of the three largest credit reporting agencies; contact information including website for the Federal Trade Commission or other federal agency that assists consumers with identify theft issues; a statement that an individual can obtain information from identified federal sources about steps to avoid ID theft; information the individual can use to contact the covered entity to inquire about the breach; and advice to the consumer to report suspected incidents of identity theft to local law enforcement or the attorney general.[75]

5.4. Penalties

The GDPR provides for penalties including administrative fines for infringement of the regulation[76] and criminal penalties are also possible.[77] Each supervisory authority has the power to impose administrative fines and identify the upper limits.[78] In the US, the laws of the 50 states may allow for civil and criminal penalties but they vary from state to state. For example, an agency that violates the Alaska statute is liable to the state for

[74]The following US states provide guidelines for the content to include in notifications of breaches: (1) Alabama Statute, *S.B. 318, Act No. 396, Consumer Protection, Alabama Data Breach Notification Act* (2018); (2) Arizona Statute, *Ariz. Rev. Stat. § 18-545 Title 18 – Information Technology: Notification of Breach of Security System; Enforcement; Civil Penalty; Preemption; Exceptions; Definitions* (2016); (3) California Statute, *Cal. Civ. Code §§ 1798.29, 1798.82: Division 3. Obligations, Part 4. Obligations Arising From Particular Transactions, Title 1.8. Personal Data, Chapter 1. Information Practices Act of 1977, Article 7. Accounting of Disclosures* (2017); (4) Colorado Statute, *Colo. Rev. Stat. § 6-1-716 Title 6 Consumer and Commercial Affairs, Notification of Security Breach*; (5) Florida Statute, 'Fla. Stat. §§ 501.171, 282.0041, 282.318(2)(i), Public Business Communications and Data Processing' (2016); (6) Hawaii Statute, *Haw. Rev. Stat. § 487N-1 et seq. Chapter 487N, Security Breach of Personal Information* (2018); (7) Illinois Statute, *815 ILCS §§ 530/1 to 530/25, Business Transactions, Personal Information Protection Act* (2006); (8) Iowa Statute, *Iowa Code §§ 715C.1, 715C.2, Chapter 715C, Personal Information Security Breach Protection* (2019); (9) Maryland Statute, *MD COMM L Code § 14-3504 Commercial Law Title 14 – Miscellaneous Consumer Protection Provisions Subtitle 35 – Maryland Personal Information Protection Act – Security Breach*; (10) Massachusetts Statute, *Mass. Gen. Laws § 93H-1 et seq. General Laws, Part I: Administration of the Government, Title XV Regulation of Trade, Chapter 93H: Security Breaches* (2018); (11) Michigan Statute, *Mich. Comp. Laws §§ 445.63, 445.72, Identity Theft Protection Act 452* (2004); (12) Missouri Statute, *Mo. Rev. Stat. § 407.1500, XXVI Trade and Commerce, Merchandising Practices, Credit Card Processing Services* (2009); (13) New Hampshire Statute, *N.H. Rev. Stat. §§ 359-C:19, 359-C:20, 359-C:21, Title XXXI Trade and Commerce, Chapter 359-C Right to Privacy, Notice of Security Breach* (2007); (14) New Mexico Statute, *2017 H.B. 15, Chap. 36, Data Breach Notification Act* (2017); (15) New York Statute, *N.Y. Gen. Bus. Law § 899-AA, N.Y. State Tech. Law 208, General Business Law, Notification; person without valid authorization has acquired private information* (2018); (16) North Carolina Statute, *N.C. Gen. Stat §§ 75-61, 75-65, Chapter 75 Monopolies, Trusts and Consumer Protection, Article 2A. Identity Theft Protection Act* (2005); (17) Oregon Statute, *Oregon Rev. Stat. §§ 646A.600 to .628, Chapter 646A — Trade Regulation* (2017); (18) Rhode Island Statute, *R.I. Gen. Laws §§ 11-49.3-1 et seq., Identity Theft Protection Act* (2015); (19) Vermont Vermont Statute, *Vt. Stat. tit. 9 §§ 2430, 2435: Title 9 Commerce and Trade, chapter 62 Protection of Personal Information* (2015) ;(20) Virginia Statute, *Va. Code §§ 18.2-186.6, 32.1-127.1:05, Title 18.2. Crimes and Offenses Generally, Chapter 6. Crimes Involving Fraud, Article 5. False Representations to Obtain Property or Credit, Breach of personal information notification.* (2017); (21) Washington Statute, *Wash. Rev. Code §§ 19.255.010, 42.56.590, Disclosure: Chapter 19.255 Personal Information—Notice of Security Breaches and Chapter 42.56 Public Records Act respectively* (2015); (22) West Virginia Statute, *W.V. Code §§ 46A-2A-101 et seq., Chapter 46A. West Virginia Consumer Credit and Protection Act. Article 2A. Breach of Security of Consumer Information.* (2017); (23) Wisconsin Statute, *Wis. Stat. § 134.98, Chapter 134 Misc Trade Regulations, Section 98 Notice of unauthorized Acquisition of Personal Information* (2018); and (24) Wyoming Statute, *Wyo. Stat. §§ 40-12-501 et seq., Title 40 Trade and Commerce, Chapter 12 Consumer Protection, Article 5 – Credit Freeze Reports* (2018).

[75]Baker Hostetler (n 64).

[76]GDPR (n 4) at Preamble Recital 148.

[77]ibid at Preamble Recital 149.

[78]ibid at Preamble Recital 150.

a civil penalty of up to $500 for each state resident that is not notified with an upper limit of $50,000.[79] In New Hampshire, injured persons shall be awarded damages of not less than $1000 for each violation and there is a maximum of $5000 in North Carolina.[80]

5.5. Definition of personal data

The GDPR defines personal data as:

> any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[81]

Some US states have a more limited definition of personal information. For example, Kansas defines personal information as

> first name or first initial and last name linked to any one or more of the following data elements that relate to the consumer, when the data elements are neither encrypted nor redacted: (1) social security number; (2) driver's license number or state identification card number; or (3) financial account number, or credit or debit card number, alone or in combination with any required security code, access code or password that would permit access to a consumer's financial account. The term 'personal information' does not include publicly available information that is lawfully made available to the general public from federal, state or local government records.[82]

5.6. Definition of data breaches

The GDPR defines a data breach as 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed'.[83] Minnesota defines a data breach as

> unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security system, provided that the personal information is not used or subject to further unauthorized disclosure.[84]

Thus, the difference between the GDPR and the Minnesota statute is 'the accidental or unauthorized loss or disclosures' of personal data versus the 'unauthorized acquisitions'. Other states add that the information is unencrypted or encrypted and the breached data includes the key. Further, for example the accidental destruction of a customer's database containing personal information would be considered a data breach under the GDPR.

[79] Alaska Statute, *AS 45.48.010 – .090 – Alaska Personal Information Protection Act Breach of Security Involving Personal Information* (2009).
[80] Baker Hostetler (n 64).
[81] GDPR (n 4) at 2016 OJ (L119/51) §1, Art 4(1).
[82] Kansas Statute, *KS Stat § 50-7a01 Consumer information; security breach; definitions. Article 7a. – Protection of Consumer Information* (2014).
[83] GDPR (n 4) at 2016 OJ (L119/51) §1, Art 4(12).
[84] MN Statute, *MN Stat § 325E.61 Data Warehouses; Notice Required for Certain Disclosures* (2016); UK Information Commissioner's Office (ICO) GDPR Guide, *Personal Data Breaches* (2018).

However, because the data was not acquired by an unauthorized source, it would be considered a breach by Minnesota law, or any other of the US laws. Also, because of the broader definition of personal data, the loss of a database of internet protocol (IP) addresses would be considered a breach per the GDPR but not per the Minnesota law. Under the GDPR, a personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorization; or if the data is made unavailable. According to the UK Information Commissioner's GDPR guidelines, personal data breaches can include: (1) access by an unauthorized third party; (2) deliberate or accidental action (or inaction) by a controller or processor; (3) sending personal data to an incorrect recipient; (4) computing devices containing personal data being lost or stolen; (5) alteration of personal data without permission; and (6) loss of availability of personal data.[85]

The UK Information Commissioner's Office (ICO) GDPR Guidelines includes the example whereby an organization uses a data processor, and this processor suffers a breach. Under Article 33(2) of the GDPR, it must inform you without undue delay as soon as it becomes aware. If the organization (i.e. the controller) contracts with an IT services firm (i.e. the processor) to archive and store customer records, and the IT firm detects an attack on its network that results in personal data about its clients being unlawfully accessed, the IT firm is to promptly notify the controlling organization that the breach has taken place. The controller organization is to notify the ICO. Further, under Article 28 of the GDPR, when a processor is used, the requirements on breach reporting should be detailed in the contract between the controller and processor. Similarly, Oregon is one state that requires a third party that maintains or otherwise possesses personal information on behalf of another shall notify the owner as soon as is practicable after discovering a breach of security.[86]

6. Conclusion

The world has become increasing smaller as global companies abound. The internet allows companies in any region of the world to have customers and thus data from any other part of the world. The essentially unlimited storage capacity means a broad array of data types can be stored. However, with the continued existence and even rise in data breaches and identity theft, consumers are increasingly a risk. The EU has made a valiant effort to address many of the vulnerabilities faced by EU residents related to their personal data. Features of the GDPR such as the obligation of data controllers to ensure that users can withdraw their consent at any time are considered innovative.[87] Yet, some critics of the GDPR have noted the lack of innovation with regard to emerging technologies such as bitcoins, pay for privacy programs and the rapidly growing personal data economy (i.e. companies that sell consumers' personal data).[88] There is also the data management and de-identification procedure called pseudonymization by which personally identifiable

[85]GDPR (n 4) at 2016 OJ (L119/49-50, 52) Chap IV §2Arts 28 and 33(2). See also Preamble Recital 87.
[86]Oregon Statute, *Oregon Rev. Stat. §§ 646A.600 to .628, Chapter 646A — Trade Regulation* (2017).
[87]Dasko (n 24).
[88]ibid; Elvy (n 14).

information fields within a data record are replaced by one or more artificial identifiers, or pseudonyms.[89]

Elvy advocates that in the new data economy in the US, personal data economy (PDE) companies must: (1) consistently implement measures to ensure that consumers maintain control over their data and proactively address past failures; (2) work with non-PDEs to significantly change the data industry; (3) prohibit pay for privacy discount programs in industries that provide digital age necessity services and products; (4) revamp the way the Federal Trade Commission (FTC) regulates data security; and (5) increase regulation of data brokers.[90] If the US were to draft a federal statute similar to the GDPR, the regulation needs to be able to address innovative business models that are on the rise.

Another issue is the size, power and influence of internet-based companies like Facebook. Monopolies need to be regulated by antitrust laws as well as data protection and intellectual property protection laws. Although Facebook resembles a monopoly, because they provide services for free, the company escapes the scrutiny of antitrust investigations.[91] This issue needs to be addressed in any comprehensive US federal statute for consumer data protection.

Similarly, the provision of social media platforms and its use is innovative. This has sparked discussions and debates about whether social media companies like Facebook should be considered media companies that need to be subjected to the same professional codes of ethics and laws that govern media companies and journalists.[92] Arguably, Facebook should not be held liable for what their customers post online and for what their customers do with the data they collect online – or should it be held liable? Thus, this is another issue that needs to be addressed in any proposed US federal statute for consumer data protection. Other innovations are in the areas of labor law. In a situation where a company has employee personal data, the GDPR does not particularly protect the employees' rights over the employers' prevailing interests.[93]

In North America, in 2000, Canada assented to the Personal Information Protection and Electronic Documents Act (PIPEDA),[94] a federal privacy law that applies to the 'collection, use or disclosure of personal information'. The US has addressed the issue of data protection on a more micro level. For example, the Health Insurance Portability and Accountability Act (HIPAA)[95] requires health entities and their business associates to provide notification of a breach of health information; and the Health Information Technology for Economic and Clinical Health (HITECH) Act[96] requires notification for a breach of electronic health records. And per the Memorandum, M-07-16 of the Office of Management and Budget, federal agencies are required to access and potentially notify individuals

[89]GDPR (n 4) at 2016 OJ (L119/51) §1, Art 4(5).
[90]Elvy (n 14).
[91]Garcia-Navarro (n 5); Aysem Diker Vanberg and Mehmet Bilal Ünver, 'The Right to Data Portability in the GDPR and EU Competition Law: Odd Couple or Dynamic Duo?' (2017) 8 EJLT; and Orla Lynskey, 'Aligning Data Protection Rights with Competition Law Remedies? The GDPR Right to Data Portability' (2017) 42 ELR 793. Lynskey argues that while the right to data portability fits nicely in the EU data protection framework, it should not be viewed as a remedy to anti-competitive concerns because data portability transactions may result in negative impacts on innovation and may actually raise barriers to market entry.
[92]Garcia-Navarro (n 5).
[93]Claudia Ogriseg, 'GDPR and Personal Data Protection in the Employment Context' (2017) 3 LLI 1.
[94]SC 2000, c5.
[95]42 USC § 1301 et seq.
[96]Enacted under Title XIII of the American Recovery and Reinvestment Act of 2009 (Pub L 111–15).

following a breach of personal information. The Gramm-Leach-Bliley Act[97] requires financial institutions to protect against unauthorized access to personal information. As of April 2018, to compensate for the lack of a federal law, all 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands passed data breach notification laws.[98]

The requirements of various laws, statutes, or regulations vary by state, country, and even audience. Companies must decide if they will base compliance on the most stringent requirements which can be financially prohibitive or meet the minimum requirements which could be managerially prohibitive. A comparison of the GDPR and the statutes related to data breach notifications reveals the types of decisions companies must make. Because the definitions of personal information and data breach vary, a company in one case would be considered to have had a breach, and in another jurisdiction would not. Companies might decide on the behalf of the consumer to notify all their customers. Because the time required to notify the consumer or some authority agency varies, a company would likely notify the entities requiring the earliest notification and continue notifications as time permits. Because penalties vary, companies might notify according to those with the costliest penalties first. Because the contents of data breach notifications are not always specified or consistent, companies would be served to develop a standard notification that would be provided to all required entities if the information is available.

This brief comparative analysis highlights the challenges companies face in trying to comply with multiple regulations. The greatest challenge exists for the small business. Just knowing the regulations would be a challenge for the small business. The GDPR may remain consistent, but the statutes of the 50 US states continue to be amended. In addition, there are the statutes of other countries. More than 100 countries have enacted data protection legislation, and several other countries are in the process of passing such laws with data protection laws.[99] Banisar has noted that data protection laws have been enacted in countries such as Thailand, Mexico, Georgia and Malaysia. The most recent US personal information security breach statutes include new laws in Arizona, South Dakota, and Alabama.[100] Thus, companies should put into place protections and personnel that would help prevent a data breach as per any of these governments' definitions in addition to a plan to comply with the existing laws of any country in which the company does business.

Disclosure statement

No potential conflict of interest was reported by the authors.

[97] 15 USC states §§ 6801–27.

[98] Ieuan Jolly, 'Data Protection in the United States' <https://content.next.westlaw.com/Document/I02064fbd1cb611e38578f7ccc38dcbee/View/FullText.html?contextData=(sc.Default)&transitionType=Default&firstPage=true&bhcp=1>.

[99] Banisar (n 49); Banisar D, *National Comprehensive Data Protection/privacy Laws and Bills 2014 Map* (SSRN 2018); United Nations Conference on Trade and Development, 'Data Protection and Privacy Legislation Worldwide' (*United Nations Conference on Trade and Development*, 2018) <https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx> accessed 19 December.

[100] F Bellamy, *Cybersecurity Legal Compliance Update: Spring 2018 Brings Sea Change to Data Breach Notification Laws* (Ryley Carlock & Applewhite 2018).