Stanford – Vienna
Transatlantic Technology Law Forum

A joint initiative of
Stanford Law School and the University of Vienna School of Law

TTLF Working Papers

No. 27

A Comparison Between Personal Data Breach Notification Requirements Under the General Data Protection Regulation in the European Union and California Laws

Natalie Karl

2017

TTLF Working Papers

About the TTLF Working Papers

TTLF's Working Paper Series presents original research on technology, and business-related law and policy issues of the European Union and the US. The objective of TTLF's Working Paper Series is to share "work in progress". The authors of the papers are solely responsible for the content of their contributions and may use the citation standards of their home country. The TTLF Working Papers can be found at http://ttlf.stanford.edu. Please also visit this website to learn more about TTLF's mission and activities.

If you should have any questions regarding the TTLF's Working Paper Series, please contact Vienna Law Professor Siegfried Fina, Stanford Law Professor Mark Lemley or Stanford LST Executive Director Roland Vogl at the

Stanford-Vienna Transatlantic Technology Law Forum
http://ttlf.stanford.edu

Stanford Law School
Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610

University of Vienna School of Law
Department of Business Law
Schottenbastei 10-16
1010 Vienna, Austria

About the Author

Natalie Karl is a 2017 graduate of Stanford Law School. She also holds a Bachelor of the Arts in Psychology from Stanford University, where she graduated with distinction. After graduating law school, Natalie plans to practice at a law firm, focusing on financing renewable energy projects.

General Note about the Content

The opinions expressed in this student paper are those of the author and not necessarily those of the Transatlantic Technology Law Forum or any of its partner institutions, or the sponsors of this research project.

Suggested Citation

This TTLF Working Paper should be cited as:
Natalie Karl, A Comparison Between Personal Data Breach Notification Requirements Under the General Data Protection Regulation in the European Union and California Laws, Stanford-Vienna TTLF Working Paper No. 27, http://ttlf.stanford.edu.

Copyright

Abstract

In May of 2018, the General Data Protection Regulation (GDPR) will take effect in the EU. The GDPR has extraterritorial applicability and will change the personal data breach notification requirements for companies doing business in the EU regardless of where the companies themselves are located. Consequently, US companies, including many technology companies located in Silicon Valley, will have to abide by these new laws. This paper addresses the similarities and differences between the personal data breach notification laws in the EU and California, as well as how any conflicts might be handled by the EU, in order to facilitate US companies' understanding of what the new EU laws will require.

Table of Contents

I. Introduction

In April 2016, the European Parliament and the Council of the European Union passed a new data privacy regulation, Regulation 2016/679, commonly known as the General Data Protection Regulation (GDPR).[1] The GDPR safeguards EU residents' right to the protection of their personal information.[2] Although the GDPR is an EU regulation, it has extraterritorial applicability and will apply to companies who are involved in the processing of personal data of individuals within the EU, regardless of whether or not the companies are located in the EU or the processing occurs there.[3] Because of this, US companies that gather and process the personal information of EU residents will have to abide by the GDPR and its provisions. However, the GDPR does not come into effect until May 2018, so it is not yet clear how some provisions of the regulation will be interpreted and enforced, or how conflicts between the GDPR and US privacy laws will be handled.[4] US companies should use the time before the GDPR becomes effective to educate themselves on its provisions and prepare themselves as best they can for its implementation.

One area of the GDPR that is important for US companies to familiarize themselves with concerns the requirements for personal data breach notifications. Currently, there is no EU law in effect that requires all companies to report data breaches; only telecommunications companies must report data breaches.[5] In the US, on the other hand, there are already a number of state laws and a few federal laws that require companies to issue data breach notifications.[6] However, because of differences between the GDPR and US laws, in particular those differences pertaining

[1] Regulation 2016/679, General Data Protection Regulation, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].
[2] *Id*. at art. 1(2).
[3] *Id*. at art. 3.
[4] *GDPR Timeline of Events*, http://www.eugdpr.org/gdpr-timeline.html (last visited Apr. 20, 2017).
[5] George R. Lynch, *EU 72-Hour Breach Notice May Give Companies Headaches*, BLOOMBERG LAW PRIVACY AND DATA SECURITY (Sept. 6, 2016), https://www.bna.com/eu-72hour-breach-n73014447213/.
[6] Ieuan Jolly, *Data Protection in the United States: overview*, THOMAS REUTERS: PRACTICAL LAW, http://us.practicallaw.com/6-502-0467 (last updated July 1, 2016).

to what personal information is covered by the laws, US companies may need to be more vigilant and careful with the personal data that they collect and process. Although US companies may already be accustomed to issuing data breach notifications, the GDPR is making big changes in EU law, and US companies will still need to prepare for it.

II. Background on Data Breach Notification Laws

There are three main issues when it comes to personal data breach notifications that companies should be aware of. First, what personal information is covered by the relevant law. Second, what constitutes a breach of this information. Third, and final, what is the required response to the breach, including any specific information that the companies are obligated to provide and any precise timelines that they are supposed to follow. The GDPR handles these three issues, particularly the first, somewhat differently from the US. Because of this, the requirements for breach notifications may vary from what US companies are used to doing under US laws.

In the US, although there are federal laws covering a few privacy concerns, such as the Fair Credit Reporting Act and the Health Insurance Portability and Accountability Act, most privacy laws, including data breach notification laws, have been enacted by the states.[7] California was the first state to enact a breach notification law, and many of the other states that have since followed suit have modeled their own laws after California's.[8] Currently, forty-seven states have data breach notification laws, along with the District of Columbia and Puerto Rico.[9] These laws tend to focus on the responses to a security breach, rather than on preventing them

[7] *Id.*
[8] *Id.*
[9] *Security Breach Notification Chart*, PERKINS COIE LLP, https://www.perkinscoie.com/en/news-insights/security-breach-notification-chart.html (last updated Mar. 2017).

from happening in the first place, although a few states, such as Massachusetts, are beginning to enact preventative statutes as well.[10] However, California is still the pioneer state in this field. It is also the home to Silicon Valley, and many California-based technology companies, as well as non-California based companies, are already familiar with and abide by California's laws. Because of this, and because these companies will have to comply with the GDPR, I will focus on how the GDPR's provisions compare to, and sometimes conflict with, California's breach notification laws.

The GDPR has extraterritorial applicability, so these provisions affect any company involved in processing the personal data of EU residents. The concept of extraterritoriality in the data privacy realm should already be familiar to many US companies that handle personal data because the US state laws they follow may have extraterritorial applicability themselves. For example, in California, the breach notification laws affect companies that do business in California and own or license computerized data that includes personal information of California residents.[11] It does not seem to matter if the company is based in California or stores and processes the data there. Therefore, like the GDPR, California's laws have extraterritorial applicability, so US companies should be used to this idea and likely already abide by multiple laws on the subject.

However, the GDPR may not always harmonize with the laws that US companies are accustomed to and, hopefully, already endeavor to comply with. Therefore, it is helpful to consider how any differences or conflicts between the GDPR and California's laws may be handled by the EU. To do so, we can look to how the EU addresses conflicts between their laws and those of a non-member state in other realms of the law with extraterritorial applicability.

[10] Jolly, *supra* note 6.
[11] Cal. Civ. Code § 1798.82 (West 2017).

Competition law, or what is known as antitrust law in the US, is one such area. Through an agreement between the EU and the US, as well as various EU court opinions, we have a sense of how the EU handles conflicts between its competition laws and those of the US. Extrapolating from this, we can get an idea of how the EU might respond to the differences and possible conflicts between the data breach notification laws of the GDPR and California.

III. The Definition of Personal Data

Before delving into the laws regarding breach notification, companies have to first know and understand what information is covered by the relevant laws. The GDPR defines personal data very broadly. It includes "any information relating to an identified or identifiable natural person." [12] The GDPR goes on to define an identifiable natural person as someone who can be identified, whether it is directly or indirectly, "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."[13] Although it is difficult to think of any personal data that does not fall into this lengthy list of information, the list is non-exhaustive, so even more information may be covered by the definition. That is, some information that is not specifically mentioned in the list would still be included. For instance, certain bits of data that companies might not currently be concerned with, such as an individual's IP address, would be protected by the GDPR.[14]

California gives personal information a similarly lengthy definition, but it is much narrower than the GDPR's. California's definition explicitly lays out what precise pieces of

[12] GDPR at art. 4(1).
[13] *Id.*
[14] Jay Cline, *Data Breach Notification: 10 Ways GDPR Differs From the US Privacy Model*, WALL ST. J. (Dec. 1, 2016), http://sponsoredcontent.wsj.com/pwc/broader-perspectives/data-breach-notification-10-ways-gdpr-differs-from-the-us-privacy-model/.

information fall into the protected category of personal data. Under California law, personal information includes combinations of a person's name with his social security number, his driver's license or state identification number, his bank account or credit or debit card number along with any passwords or security codes, his medical information, his health insurance information, or information collected through an automated license plate recognition system.[15] Further, an individual's user name or email address, along with any required password or security questions and answers, would also be considered personal information.[16] The definition excludes any publicly available information.[17] California's definition may be long, but it is extremely specific, and it is exhaustive.

The GDPR's definition of personal data is significantly broader than California's. It is essentially any information that can be used to identify a person, regardless of whether this information is typically kept private, such as a bank account number, or is typically public, such as an individual's physical characteristics. It seems that all information collected from a person could be included in the GDPR's personal data definition somehow, whereas very little information would be covered by California's definition. California's law only covers a specific set of information that seems focused on particularly sensitive personal information that is normally kept completely private, and that, if leaked, could be used to commit some sort of crime, such as identity theft, blackmail, or extortion. Every part of California's definition would be covered by the GDPR, but California's definition is silent on much of the information included in the GDPR, such as cultural or social identity. Because the GDPR's current definition of personal information is so vague and broad, particularly in comparison with California's, and it is not clear how it will be interpreted yet, California companies should familiarize themselves

[15] Cal. Civ. Code § 1798.82(h)(1) (West 2017).
[16] *Id.* § 1798.82 (h)(2).
[17] *Id.* § 1798.82 (i)(1).

with the GDPR's definition, clarify what information they collect from people, and be more careful with that information.

IV. What Constitutes A Data Breach

Moving on from the definition of personal data, the next step for a company to take is to look at how a data breach is defined. Fortunately, in this realm the GDPR and California are on the same page, so US companies should already be familiar with the concepts covered by the law. In the GDPR, a personal data breach is "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."[18] In California, a data breach means "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business."[19] These two definitions are more harmonious than the definitions of personal data; each is focused on the security of the information and unauthorized access to it. However, because the GDPR includes so much more in its definition of personal data, its breach definition will necessarily cover more than what US companies are used to.

V. Breach Response

Once a company is aware of a data breach affecting the personal information at issue, it has to know how to respond to the breach. The GDPR's breach notification provisions concern the responsibilities of two entities, the controller and the processor. The controller is the "person, public authority, agency, or other body" that determines the purposes and means of personal data

[18] GDPR at art. Article 4(12).
[19] Cal. Civ. Code § 1798.82(g) (West 2017).

processing, and the processor, unsurprisingly, actually processes the data for the controller.[20] Additionally, each member state must also create a supervisory authority to monitor the application of the GDPR.[21] The GDPR has two separate provisions concerning breach notification: Article 33 regarding notifying the supervisory authority, and Article 34 regarding notifying the data subject. Both provisions are relevant to US companies handling the personal data of EU residents.

In contrast, California does not have a supervisory authority or anything like it, and so it is particularly concerned with notifying the individuals whose data was breached. However, it also has two provisions regarding breach notification: California Civil Code Sections 1798.29 and 1798.82. Section 1798.29 is essentially the same as Section 1798.82 but for agencies, rather than persons or companies. Because there are no significant substantive differences between the two, I will focus on the language from Section 1798.82 referring to companies.

A. Who Is Notified

The first thing a company has to know when it learns of a breach is whom it will need to notify. The GDPR splits its notification provisions by the recipient of the notification; Article 33 concerns the supervisory authority, and Article 34 concerns the data subjects. With respect to the supervisory authority, the controller does not have to issue a notification if "the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons."[22] Similarly, the controller need only communicate the data breach to the data subjects when the breach "is likely to result in a high risk to the rights and freedoms of natural persons."[23] This is a slightly

[20] GDPR at art. 4(7)-(8).
[21] *Id.* at 51.
[22] *Id.* at 33(1).
[23] *Id.* at 34(1).

more stringent standard than that for notifying the supervisory authority because it requires a "high" risk, rather than just a risk, so it is possible that in some cases the controller may need to notify the supervisory authority but not the data subjects. The controller also does not need to notify the data subjects of the breach if he appropriately protects the personal data at issue in the breach, such as by encryption, takes measures to ensure that the high risk to the rights and freedoms of the data subjects is no longer likely, or could only notify the subjects with disproportionate effort, in which case he must issue a notification via a public communication.[24] However, even if the controller believes that no notification of the data subjects is necessary, the supervisory authority may order him to notify them anyway.[25]

On the other hand, because there is no supervisory authority in California, the breach notification provisions of the law concern notifying the California residents affected by the breach. [26] A company need only issue such a notification if it believes that an unauthorized person acquired the resident's unencrypted data or the resident's encrypted data along with the encryption key.[27] However, if the notification must go to more than 500 California residents, then the person or company issuing the notification must send a sample notification to the Attorney General.[28] This provision is likely concerned both with assuring the adequacy of the notification and with notifying the Attorney General of the breach in the way that the GDPR requires notifying the supervisory authority. Chances are that in most cases, particularly those breaches that are the result of a hacking, more than 500 California residents will need to be notified, so companies are probably accustomed to sending their notifications to the Attorney General already. Therefore, while under the GDPR a company may need to notify the

[24] *Id.* at 34(3).
[25] *Id.* at 34(4).
[26] Cal. Civ. Code § 1798.82(a) (West 2017).
[27] *Id.*
[28] *Id.* § 1798.82(f).

supervisory authority but not the data subjects, in California a company will always have to notify the data subjects, if it has to notify anyone at all.

Because California has a much narrower definition of personal data, there is a limited set of data breaches that would trigger its notification provision. The standards in the GDPR, however, are not as clear, and because of the broad definition of personal information, the sheer amount of data at issue is much larger than it would be in California. To illustrate, determining the likelihood that people's rights and freedoms will be risked is an inherently fuzzy standard. It is not always clear how the personal information at issue relates to the individual's rights and freedoms, such as in the case of some physical identifiers, nor is it clear what would constitute a risk of those rights and freedoms, or just how likely that risk would have to be to be covered by the GDPR. There are easy cases, such as a breach of people's unencrypted financial information, but given how broad the definition of personal data is, there will be many questionable cases. It may vary, depending on how sensitive the information from those identifiers is viewed, which may depend on whether or not people would view it as something private, like one's health information, or something more public, like one's physical appearance. Certain types of information breaches, perhaps like some cultural or physical identifiers, might not risk everyone's rights and freedoms, but they may for a particular person or group of people if that information is usually somewhat private and others may make judgments based on those identifiers. For instance, revealing someone's ethnic origin may be harmful to that person if he is a member of a marginalized group and may suffer prejudice as a result of the revelation. It is not clear how these provisions of the GDPR will be interpreted yet, but companies should be aware that some information that they collect that they might not view as personal enough, or that they

might not think is linked to people's rights and freedoms, may actually be included in the GDPR and be subject to these breach notification provisions.

B. Timing of the Notification

The second concern for a company who needs to respond to a breach of personal data is timing. A company has to know how quickly it must send out any notifications after learning of a data breach. Although anyone that might be affected by a data breach would want to know as soon as possible, the more time a company can take to send out the notifications, the more information it can gather on the breach and share with the relevant parties. If the company has to make a snap judgment about whether or not to issue a notification, then it may only be able to share that there was a breach without any specifics, which could invite a lot of questions and could be very unsatisfactory for anyone affected by the breach.

The GDPR seems to be taking the position that companies need to issue their notifications quickly. According to the GDPR, in the event of a personal data breach that requires notifying the supervisory authority, the controller must do so "without undue delay and, where feasible, not later than 72 hours after having become aware of it."[29] Any notifications after 72 hours must "be accompanied by reasons for the delay."[30] If, on the other hand, the processor of the data discovers the breach, then it must notify the controller "without undue delay," but there is no set period of time.[31] At that point the controller will have to decide whether or not it has to notify the supervisory authority. The controller must also communicate the personal data breach to the data subjects it affects "without undue delay."[32] Additionally, recall that even if the

[29] GDPR at 33(1).
[30] *Id.*
[31] *Id.* at art. 33(2).
[32] *Id.* at art. 34(1).

controller does not believe that the breach constitutes a high enough risk to the rights and freedoms of the data subjects such that it needs to notify them, the supervisory authority may order it to do so.[33]

This part of the GDPR is rather ambiguous. It is unclear whether or not the 72 hour requirement is really a requirement or a suggestion, and, if it is a requirement, how much information companies are expected to report at that time.[34] The regulation says that the controller must issue the notification "where feasible" no more than 72 hours after becoming aware of the breach.[35] This does not necessarily sound like it is required for the controller to issue a notification within 72 hours, but, reading on, the GDPR adds that if a notification does not get out within 72 hours, then it must "be accompanied by reasons for the delay."[36] This does make it sound like the 72 hour window is a requirement and not a suggestion. Such a short window may be all right as long as the supervisory authorities do not expect much information from the preliminary notification.[37] For instance, it may be difficult to determine the consequences of a breach within that time period if it is not clear precisely what information was leaked, which is often the case if a company is hacked.[38] It is also possible that putting together an appropriate notification so quickly may mean that other things, such as corrective actions to mitigate the risk of harm, may be put on the back burner. [39] If this is interpreted as a requirement, it will be a difficult one for companies to meet satisfactorily.

Moving over to California, there are no strict time requirements under the law. A company that discovers a personal data breach that will require notifying the affected California

[33] *Id.* at art. 34(4).
[34] Lynch, *supra* note 5.
[35] GDPR at 33(1).
[36] *Id.*
[37] Lynch, *supra* note 5.
[38] *Id.*
[39] *Id.*

residents must issue that notification "in the most expedient time possible and without unreasonable delay."[40] Just as the processor must notify the controller under the GDPR, anyone who maintains computerized personal data must notify the owner or licensee of the information of the breach immediately.[41] However, if a law enforcement agency determines that the notification of the breach will interfere with a criminal investigation, then notification may be delayed until the law enforcement agency determines that notification will not compromise the investigation.[42] If this happens, then the company must disclose the reason for the delay when it does finally issue the notification.[43] However, that is the only time a company needs to explain why a notification was delayed under the statute, probably because it is the only time a company is legally allowed to delay notification.

Assuming that the GDPR's 72 hour window is interpreted to be a strict requirement, the GDPR has a specific timeframe for notifying the supervisory authority, but California only has the indeterminate standard of "without unreasonable delay." This may end up conflicting with the 72 hour requirement, particularly if California is delaying notification to gather more information. For example, if a California company is aware of a breach that would require notifying the supervisory authority under the GDPR, regardless of whether or not the data subjects need to be notified as well, but the company has been told to delay notification in California by a law enforcement agency, it is not clear what it should do. Issuing the notification may get the company in trouble in California, and not issuing it may get the company in trouble in the EU. If the company need only notify the supervisory authority and can do so confidentially and postpone notifying the data subjects, then it may be able to do so without flouting the

[40] Cal. Civ. Code § 1798.82(a) (West 2017).
[41] *Id.* § 1798.82(b).
[42] *Id.* § 1798.82(c).
[43] *Id.* § 1798.82(d)(2).

California law enforcers and impeding their investigation. However, this will depend on the level of risk, whether or not the company is obligated to notify the data subjects under the GDPR, whether the supervisory authority orders them to notify the data subjects, and, if so, whether the supervisory authority allows them to delay notification. If may also be that delaying notification to the supervisory authority for a law enforcement investigation would be a sufficient reason to wait more than 72 hours, particularly if that investigation would benefit the EU and its residents. The short timeframe will require companies to make quick decisions regarding notifications, so they should prepare a protocol for when a data breach occurs after the GDPR has come into effect, rather than wait and see what happens.

C. Notification Requirements

Once a company has determined that a personal data breach notification is necessary, both the GDPR and California have various requirements for what that notification must contain. Under the GDPR, the notification is required to contain at least four pieces of information: a description of the nature of the breach, including the categories and approximate number of data subjects and data records concerned; the name and contact information of the data protection officer; a description of the "likely consequences" of the breach; and a description of the steps the controller has taken or will take to address the breach, including mitigation measures.[44] For notifications going out to the data subjects, the description of the nature of the breach must be in "clear and plain language."[45] If the controller could only notify the subjects with disproportionate effort, then he must notify them via a public communication.[46]

[44] GDPR at art. 33(3)(a)-(d).
[45] *Id.* at art. 34(2).
[46] *Id.* at art. 34(3)(c).

California has more requirements for what needs to be included in the breach notification than the GDPR. First, the notification can be written or electronic.[47] As previously mentioned, the person or company issuing the notification must send a sample of the notification to the Attorney General if the notification is going to go to more than 500 California residents.[48] If providing notice would cost more than $250,000 or over 500,000 people must be notified, then the company may provide substitute notice, which includes "[c]onspicuous posting" on the company's website for at least 30 days, notifying "major statewide media," and emailing notice when they have the email addresses for the individuals affected.[49] The notification must "be written in plain language," be titled "Notice of Data Breach," and include specific information under specific headings.[50] There are also format requirements and minimum font size requirements, presumably designed to make it clear to the average person what the notification is about.[51] The statute itself contains a "model security breach notification form," which if filled out in plain language will comply with the notification requirements.[52] There are also information requirements for the notification, including the name and contact information of the reporting person, what type of personal information was acquired, when the breach occurred, whether notification was delayed because of law enforcement, a description of the breach, contact information of major credit reporting agencies if social security numbers or driver's license were acquired, and an offer to provide "appropriate identity theft prevention and mitigation services" for at least a year.[53]

[47] Cal. Civ. Code § 1798.82(j)(1)-(2) (West 2017).
[48] *Id.* § 1798.82(f).
[49] *Id.* § 1798.82(j)(3).
[50] *Id.* § 1798.82(d)(1).
[51] *Id.*
[52] *Id.* § 1798.82(d)(1)(D).
[53] *Id.* § 1798.82(d)(2).

California's requirements are generally more stringent than those of the GDPR, so a notification that meets the California law requirements would likely also meet the GDPR requirements. However, there could be some confusion over what qualifies as a description of the consequences of the breach because California does not have this requirement. California's law skirts this issue by requiring a description of what information was taken and identity theft protection services. This difference is probably because the personal data at issue in California law is a narrow subset of information that could be used to steal someone's identity or commit another crime, whereas the GDPR includes much more in its personal data definition, so the information is not already inherently linked with identity theft and could have different consequences. Therefore, this would likely be an issue in cases where there was a breach of personal information covered under the GDPR but not the California Code, such as a breach of social or cultural identity information. It is unclear what the consequences of a breach of this type of information would typically be, and so this may be a more fact-specific, laborious inquiry to undertake.

VI. Differences and Potential Conflicts Between the GDPR and California Law

Although the personal data breach notification laws of the EU and California are fairly similar, there are a few areas with fairly significant differences. First, the GDPR's definition of personal data is so much broader than California's that companies may not even realize that the information at issue in a data breach falls into this category. For example, when there is a breach that only reveals information relating to individuals' ethnic backgrounds. A company may maintain that a breach of this sort of information is not necessary to report because it is unlikely to risk anyone's rights or freedoms, even if it might cause problems for someone belonging to a

marginalized group that suffers a lot of prejudice. Therefore, in the company's eyes, a notification of this sort of breach will not really help people in any way, and it could waste time and resources, as well as damage the company's reputation, if it must report all such insignificant breaches. Second, the GDPR's requirement that the data controller must notify a supervisory authority within 72 hours, unless there is a valid reason for the delay, is stricter than California's laws, and there may be conflicts when law enforcement agencies in the US want to keep the breach confidential and prevent a notification from going out. Third, the breach notification requirements are slightly different, particularly when it comes to describing the consequences of the breach, which could prove difficult for US companies who struggle to see why some information is covered by the GDPR.

Given that the GDPR will not come into effect until May of 2018, companies have some time to figure out how to comply with its provisions. However, particularly in the case of the 72 hour window for notifying the supervisory authority, complying with the GDPR may conflict with complying with California Law. It is also likely that other provisions in the GDPR conflict with California or US law, but it is unclear how these conflicts will be handled. One area of law that has already seen conflicts between the EU and the US is competition law. In order to understand how the EU might handle conflicts with US law, we can look to the competition laws.

A. Conflicts in the Competition Laws Between the EU and the US

Like the GDPR, the EU's competition law has extraterritorial applicability. EU law covers companies that are established outside of the EU, but that produce goods that are then

sold within the EU. [54] For instance, if a group of these companies collude on the prices they charge EU customers, and they actually do charge their EU customers based on this price coordination, then this will restrict, and is clearly intended to restrict, competition within the EU in violation of Article 101 of the Treaty on the Functioning of the European Union.[55] The European Commission thus has territorial jurisdiction to proceed against the companies, even though they are located outside of the EU.[56]

Because of this extraterritorial applicability and in order to deal with potential conflicts, the US and the EU entered into an agreement on September 23, 1991 regarding the application of their respective competition laws.[57] This agreement is intended "to promote cooperation and coordination and lessen the possibility or impact of differences between the Parties in the application of their competition laws."[58] As part of the agreement, each party is required to notify the other when they become aware that their enforcement of competition laws "may affect important interests of the other party."[59] The parties also agree to exchange information about their competition laws and enforcement, including by meeting at least twice a year to keep each other up to date.[60] Further, the parties agree to assist the other party's enforcement of its competition laws, as long as they are compatible with the assisting party's laws.[61] The most relevant part of this agreement for our purposes is Article VI regarding avoiding conflicts. In a nutshell, each party agrees to "take into account the important interests of the other Party," including when deciding whether or not to investigate, initiate proceedings, or implement

[54] Case C-231/14 P, Innolux v. Commission, 2015 EUR-Lex CELEX LEXIS 62014CJ0231 (July 9, 2015), P 72.
[55] *Id.*
[56] *Id.*
[57] Agreement on the Application of Their Competition Laws, EU-US, Sept. 23, 1991, 30 I.L.M. 1487 (1991).
[58] *Id.* at art. I(1).
[59] *Id.* at art. II(1).
[60] *Id.* at art. III.
[61] *Id.* at art. IV(1).

remedies or penalties.[62] When it seems that the enforcement activities will have an adverse effect on the other Party's interests, the Party may take into account specific factors, such as the relative significance of the activities at issue and their effects within the two separate territories.[63]

Since the agreement was concluded, the European Court of Justice has issued decisions about cases in which there have been conflicts between the laws of the EU and the US. Although the agreement says that the EU will take into account the interests of the US, the court has said that "a legal position adopted by the law of a third country cannot take precedence over that adopted by EU law and that an infringement of that law does not constitute as such a defect resulting in the illegality of a decision adopted under EU law."[64] The Court has also found that the United States law "cannot take precedence over that adopted by European Union law."[65] The court will take note of any legal battles going on in the United States, as well as any settlements arising from those cases.[66] However, even if the case in the United States was resolved, whether by settlement or court case, that does not mean that the EU case is no longer valid.[67] Therefore, the EU laws will pretty much always apply in competition cases, even though the EU considers the US, its laws, and the effect of the case on the US.

B. Application to the GDPR

Although it would be beneficial if the EU and the United States were to enter into an

[62] *Id.* at art. VI.
[63] *Id.* at art. VI(3).
[64] Case T-472/13, Lundbeck v. Commission, 2016 EUR-Lex CELEX LEXIS 62013TJ0472 (Sept. 8, 2016), P 511.
[65] Case T-321/05, AstraZeneca v. Commission, 2010 EUR-Lex CELEX LEXIS 62005TJ0321 (July 1, 2010), P 368 (where both sides attempted to argue that United States law bolstered their positions).
[66] Case T-201/04, Microsoft v. Commission, 2007 EUR-Lex CELEX LEXIS 62004TJ0201 (Sept. 17, 2007), P 51-55 (where the court discussed Microsoft's litigation with the Department of Justice and eventual settlement).
[67] *Id.* at 973-74 (where the court found that Microsoft's settlement with the DOJ was too limited in time and in scope to address all of the violations and remedy the abuse).

agreement regarding their data protection laws, as they did with the competition laws, it may be more difficult to come up with such an agreement because the US and the EU are so different with respect to their concerns about privacy. One need only look to the wildly differing definitions of personal data to see this. It would also be beneficial to know first how the provisions of the GDPR were going to be interpreted before entering into any agreements. However, even without a written agreement, many of the same ideas from the competition law realm will likely apply.

California law will not take precedence over EU law, and it will have limited applicability in cases arising under violations of the GDPR. However, the EU may be willing to take into account the interests of the United States when assessing the violations of the GDPR. For instance, in the event of a breach where notification is delayed so as to prevent impeding an investigation by a law enforcement agency, the EU courts may be willing to consider that interest. That is, the law enforcement purpose of the delay may constitute a valid reason for not notifying the supervisory authority within 72 hours. This sort of delay may also be within the interests of the EU because the investigations may help them as well. US companies would do well to share the information that they can with the EU when this happens. Even if this does not constitute a valid reason and the supervisory authority should have been notified, it may be an appropriate reason to keep the notification to the supervisory authority confidential and delay notifying the affected residents.

With respect to the differences between the definition of personal data and the information included in the breach notifications, it is difficult to say what the EU will do before knowing how these provisions will be interpreted. As in competition law, the EU will not let California's definition of personal data take precedence over the GDPR's definition. This may be

more or less of a problem depending on whether or not all of the information included in the GDPR requires a notification. The effect of this will then cascade down into the information disclosed in the breach notifications. If the only information that triggers notifications is similar to that in California law, it will not be an issue. However, and more likely, if more types of personal information trigger the notification provisions, then companies will have to translate that information and the consequences of its release into their notifications. The EU law will still rule the day.

VII. Consequences of Violating the GDPR

US companies would do well to think through how they might respond to data breaches before the GDPR becomes effective because of the potential consequences of violations. For violations of Articles 33 or 34, a supervisory authority may impose an administrative fine of up to the higher of either 10 million Euros or "2% of the total worldwide annual turnover of the preceding financial year."[68] For many Silicon Valley companies, this could be a massive amount of money. In assessing the fine, the supervisory authority can take into account a number of considerations, such as the gravity of the violation, any mitigation action on the part of the controller or processor, or the type of personal data affected.[69] Further, this fine can be in addition to or instead of other corrective actions on the part of the supervisory authority, such as issuing warnings or reprimands, or imposing a ban on processing.[70] Because the interpretation of the GDPR is currently unclear, and because the supervisory authority can take into account a company's actions when assessing a fine, a company would do well to document its risk assessment procedures and how it determines whether or not to notify the supervisory authority

[68] GDPR at art. 83(4).
[69] *Id.* at art. 83(2).
[70] *Id.* at art. 58(2).

and the data subjects.

VIII. Conclusion

The GDPR and California handle data breach notification requirements differently. Each defines personal data very differently, which may lead to conflicts between the laws in the future. That is not the only difference between the two laws, as the timing requirements may come into direct conflict, depending on how strictly the GDPR is interpreted. However, regardless of how strictly the GDPR is interpreted, even if the EU considers the US interests and laws when deciding if a US company violated the GDPR, the EU law will still take precedence over any US laws. Preparation will be very important when it comes time for companies to make quick judgments, and better documentation will likely help the companies if there are any possible violations of the GDPR. Because of this, US companies should familiarize themselves with the GDPR, including its data breach notification provisions, and create a well-documented plan for the event of a data breach once the GDPR comes into effect.