International Relations and Diplomacy, June 2020, Vol. 8, No. 06, 231-239
doi: 10.17265/2328-2134/2020.06.001

U.S. and International Legal Perspectives Affecting Cybersecurity Corporate Governance

Paul J. Morrow, Thomas M. Fitzpatrick
Husson University, Bangor, USA

International and U.S. corporations must be well advised regarding specific regulations and laws that affect cybersecurity decisions because the Board of Directors must perform due diligence to avoid regulatory negligence and lawsuit liability. Depending on the standards and the regulations that do define reasonable care, the corporate director is faced with the challenge of determining how and what cybersecurity laws apply. Then, directors can institute best cybersecurity management practices. This paper provides guidance regarding the application of the law in the areas of cyber security for the international corporations interacting with the European General Data Protection Regulations (GDPR), the California Consumer Privacy Act (CCPA), and recent Federal Trade Commission (FTC) administrative agency rulings. Reading this paper is worth your time because it will inform you of the legal challenges that international and domestic corporations face in making decisions about spending capital to manage cybersecurity and at the same time perform due diligence. In other words, if there is a cybersecurity breach, this paper will provide insights into what law must be followed by the corporation enabling the best management decisions assuring adequate response, compliance, thereby avoiding unnecessary liability risk. The paper also provides reflections about whether the GDPR serves as a better legal comprehensive regulatory model rather than the recently enacted laws in the U.S.

Keywords: cybersecurity compliance, General Data Protection Regulation, California Consumer Privacy Act, data privacy, Federal Trade Commission

Global Regulation of Cybersecurity

Cybersecurity corporate law involves the internal regulatory process that corporations use to govern the way to operate business domestically and internationally. The government promulgates regulations that provide the legal framework for corporations. In cybersecurity corporate law, there is a dilemma. On the one hand, the U.S. legal system has made patchwork of cybersecurity corporate governance. For example, the courts and thus the common law have its own interpretations of the doctrinal aspects of cybersecurity corporate law. In the common law, where cases are decided on a case by case basis, cybersecurity law takes on a whole different meaning and interpretation than the traditional law of contract in an arm's length transaction, person to person. Adding to the uncertainty of the common law, the regulatory agency, the Federal Trade Commission (FTC), is a specialty regulatory body that has the authority to govern commerce in the U.S. As expected, the FTC has its own

Paul J. Morrow, Dr., Sr., J.D., Esq., Associate Professor, School of Business and Management, Husson University, Bangor, Maine, USA.
Thomas M. Fitzpatrick, Dr., DBA, Professor, School of Business and Management, Husson University, Bangor, Maine, USA.

interpretation of cybersecurity law. In the European zone, the EU regulates cybersecurity implementing the General Data Protection Regulations (GDPR). Corporations have their own internal interpretations of cybersecurity policy. International firms based in different countries around the world have their versions of cybersecurity policies. Finally, different countries have their own laws on cybersecurity that vary and are much different from U.S. law. International corporations doing business across the globe face huge international business management challenges navigating the landscape of cybersecurity. In some cases, international corporations who have the best intentions are subjected to the perception of corruption issues when operating their corporations. The differences in cybersecurity law and regulations give rise to the perception that international corporations are constantly trying to circumvent the law when they are doing their best to comply with laws that they do not know. The problem is that the law of cybersecurity corporate law is confusing, and unknown, subject to wide interpretations. There is little guidance and consistency for international corporations. As a result, businesses face inconsistent compliance requirements and inordinate risk. As one possibility, the principles covered in the GDPR may suggest a better, more consistent compliance approach to cybersecurity corporate law governance.

> The General Data Protection Regulation (GDPR)—Europe's most comprehensive data privacy law to date—turned the digital world on its head when it became enforceable on May 25, 2018. Although rooted in European Union (EU) law, the reach of this landmark data protection and privacy regulation far exceeds the physical boundaries of the EU, and the European Economic Area (EEA) and Switzerland (hereafter referred to as EEA for brevity). This most notably includes the United States (US), the biggest trading partner of the EU. The wide reach of the GDPR naturally raises a few questions: Does the GDPR apply to US businesses? Does it apply to US citizens? How is the GDPR enforced in the US? How does it differ from other privacy laws in the US? (Sabastian, 2019)

Facebook and other international corporations have faced the scruples of the GDPR. The news about the violations of the GDPR and the fines faced by companies like Marriott, and British Airways have dominated the headlines. Fines for cybersecurity violations have run in the hundreds of millions of dollars. This being the case, the GDPR is already important in its application to American cybersecurity legal interpretations and for other international firms.

> … the GDPR applies to the US (and all other countries worldwide). This is because, Article 3 of the GDPR, which defines the law's territorial scope, states that it not only applies to companies in the EU/EEA, but also to companies outside of the EU/EEA that serve (or track the data of) EU/EEA residents. (Sabastian, 2019)

Any U.S. business that sells or who's primary target attracts customers (website) from the EU/EEA or the primary purpose is to tract data from the EU/EEA the GDPR applies. If the website is informational or the primary target (purpose) is not, then the GDPR does not apply. If a U.S. based company is doing business in the EU/EEA, GDPR applies. To the New York merchant who has a website selling merchandise in the EU/EEA, the GDPR would apply. The questions of applicability are directly relevant to (targeted EU/EEA) associated activity. For example, a restaurant gathering and storing data in the U.S. would not invoke the GDPR. A U.S. merchant selling to European businesses would invoke the GDPR.

> Depending on where they are located, the GDPR can and does apply to US citizens. The GDPR uses the term data subject to refer to the individual whose data is being processed. Per most interpretations of the GDPR, whether the GDPR applies is dependent on where the data subject is when their data is processed, and not the citizenship or nationality of the data subject. Therefore, the GDPR would apply to US citizens if/when they are located in the EU/EEA, but not those located in the US.

> The GDPR does not make blanket exceptions to governmental or public agencies. Therefore, if the US government targets or processes the personal data of EU/EEA-based users, it will be expected to comply with the GDPR. This is true for all non-EU/EEA public agencies. (Sabastian, 2019)

Like anything else, compliance costs within corporations run high. Security compliance audits take time, effort, and money with many issues going unresolved. Government agencies, with fine imposing authority, are like watchdog organizations policing and chasing a spirit that they themselves do not understand. To corporations, a fine does little good within the company except place incredible pressure on the e-marketing and IT departments because standards of compliance are poorly defined and many times unreasonable. In any event, we must march on, directors feeling the pressure of having to do something rather than nothing even if no one understands. In an ancillary way, corporations who are under watch from the distance do benefit in some ways. To the corporations and administrative government agencies struggling, the GDPR in the way of clarity and productivity has more to offer than compelled blind compliance. It's like your mother asking you to do something. You know you must do it. But, you do not know how to do it or why. In any event, businesses must move on whether they are compliant or not.

Compliance has its virtues. It forces a person to do things that they might not ordinarily do. For one reason or other corporations must adapt. This is the reality of the present time. With COVID, new technology, redefined markets, new consumer tastes and preferences, and a completely different legal landscape, today's business must change for the better in a constantly evolving business environment. Privacy demands are great, and the government must do something to improve accountability. The best way for a governing body to make a point and be noticed is to impose penalties and fines on corporations who do not comply. Ultimately by doing something, the whole business consumer cycle improves. At least, that is the goal.

> However, the problem with concentrating on the punitive side of the GDPR is neglecting new business opportunities. The real driver for adopting new compliance principles should be to make your business more efficient, secure and competitive. Let us take a look at some of the carrots that many may leave out while scaremongering about GDPR sticks.
>
> Benefit One: Enhance Your Cybersecurity: There is no company in the world that can afford to take the risk of cybersecurity ignorance, given the costs of data breaches and business downtime caused by theft or loss of critical data. It does make sense to take data privacy seriously and the GDPR can help you establish a security-conscious workflow.
>
> Benefit Two: Improve Data Management: To be compliant, you should know precisely what sensitive information you hold on people. Obviously, the first thing you want to do for your GDPR compliance is to audit all the data you have. This will enable you to minimize the data you collect and hold, better organize storages and refine data management processes.
>
> Benefit Three: Increase Marketing Return On Investment (ROI): One of the key principles of the GDPR is that the organization should implement an opt-in policy and have a data subject's consent to process their personal data. Combined with purging irrelevant ROT information stalling your marketing, such as lost leads or unengaged addresses, you will receive a lean fine-tuned database of highly relevant leads and customers that genuinely want to hear from you. With this information at hand, you will be able to experiment with niche marketing by tailoring your message to the specific needs and habits of a clearly defined audience that has more interest in your brand.
>
> Benefit Four: Boost Audience Loyalty and Trust: GDPR compliance can support your business in helping you build more trusting relationships with your customers and the public generally. When gathering consents to use data subjects' data, you will have to explain clearly and concisely how you will be using their personal information. Since consumers are becoming more and more suspicious about how their data is handled, the transparency and responsibility you demonstrate will encourage trust in your brand. Thus, you can use the GDPR to underline that you do care about the privacy of your current and prospective customers and stand head and shoulders above your competitors.
>
> Benefit Five: Become the First to Establish a New Business Culture: There is nothing new about businesses being animal-friendly, eco-friendly, LGBT-friendly, though 10-15 years ago it seemed impossible. Why not become human

> privacy-friendly? Organizations should think of their brand as a decent human being that doesn't just consume to sustain itself and grow but also contributes to the community. (Fimin, 2018)

All of these benefits accrue from the GDPR. One hopes that in the long run, businesses become more efficient, and have better rubrics for better performance that ultimately translate into increased accountability, better cash flow, higher profitability, and substantial growth. Although growth never comes easy, consumers remain the driving force behind the demands for better management, especially from the international sector. The GDPR gives the consumer information about how their personal data is being used. Most companies under the GDPR rubric are not allowed to sell the data which helps to build trust between the consumer and the corporation. Internal protections are implemented to better safeguard consumer data. For example, firewalls and other security measures are used to ensure that the consumer information is not accessed by hacking. If a system is penetrated, companies must give notice to the consumer in a quick and timely manner that includes actual notice of the breach within 72 hours. Finally, privacy and reasonable care of consumer information must become a legitimate top priority. We all know that matters that do not have an immediate effect on the bottom line get pushed off onto the back burner while managers and executives solve the productivity and profitability issues first. Now, the ancillary perspective of privacy becomes an issue that corporations must address in the normal day to day operational management of a company or face severe and dire consequences of a regulatory audit after a data breach that can compromise the company for years.

Comparison of Global Regulations of Cybersecurity With the U.S.

As the GDPR creates management challenges with global implications, most companies around the world are reviewing their privacy policies and instituting consent practices. Companies no longer can use personal data without the consent of the consumer. The consumer is given an opportunity to agree or opt out of the practice of allowing a company shared data privileges. This precept is viable within the provisions of the GDPR and the new California Consumer Privacy Act (CCPA) recently enacted to protect the consumer. In some ways, because the Europeans were first to respond with the GDPR, regulatory corporate compliance became the great news of the day. After much trepidation and concern, California passed its own law, the first of its kind in the nation. The CCPA essentially provides that corporations cannot sell personal data and indeed must protect the personal data of its customers. If there is a data breach, the company is accountable. Consequently, corporations must take cybersecurity very seriously.

> California was one of the first states to provide an express right of privacy in its constitution and the first to pass a data breach notification law, so it was not surprising when state lawmakers in June 2018 passed the CCPA, the nation's first statewide data privacy law. The CCPA isn't just a state law—it will become the defacto national standard for the foreseeable future, because the sheer numbers of Californians means most businesses in the country will have to comply. The requirements aren't insignificant. Companies will have to disclose to California customers what data of theirs has been collected, delete it and stop selling it if the customer requests. The fines could easily add up—$7,500 per violation if intentional, $2,500 for those lacking intent and $750 per affected user in civil damages. (Sirota, 2019)

This does set up a classic comparison between the CCPA and the GDPR. We already know to whom both laws apply. Important to note that at the inception of the GDPR, there was international business resistance. Now cybersecurity statutes and regulations have better acceptance. The letter of the law and the scope of the law do matter.

> You probably remember all the hubbub around the General Data Protection Regulation (GDPR) when it was introduced in May, 2018 in Europe. Although GDPR was a huge step forward toward preventing companies from selling the consumer data they collect, it had its critics. And companies affected by the law lamented the time and cost of compliance, as well as the potential fines that could be levied against them if they failed to comply: A business can pay up to $23.5 million, or 4% of their global annual revenue. But these high-stakes consequences have forced EU companies to take cybersecurity very seriously—and that much is a good thing. (Fertik, 2020)

In some ways the CCPA, which applies if a corporation is doing business in California, is similar to the GDPR. The GDPR has a wider scope of application in that all U.S. international corporations doing business in Europe are subject to the GDPR, including California. The CCPA, even though the law applies to corporations that conduct business in one state (California), is still a step in the right direction for the many reasons outlined.

> With the CCPA, the Consumer's in charge: Although no two laws are quite similar, the CCPA differs from the GDPR in a few important ways:
>
> - Business impacted: Whereas businesses of any size must comply with the GDPR, the CCPA only impacts businesses that reach a certain size who process a certain amount of data.
> - Fines: GDPR fines are capped based on a business's annual revenue, whereas CCPA fines have no ceiling and are assessed per violation.
> - Opt-in/Opt-out: Under the GDPR, businesses must have opt-in from consumers prior to collecting data, whereas with CCPA, consumers must opt-out of data collection.
> - Third-party data sales: Under GDPR, businesses must have consent from customers before and third-party processing or sales of data, while the CCPA requires businesses to simply notify the customer of a data sale or transfer and give them the opportunity to stop it.
>
> In short, CCPA actually puts consumers in the driver's seat. It's up to consumers to take action if they want their data to remain private—but businesses are required to heed their requests. (Fertik, 2020)

The answer to the many breaches of security and the public use of consumer private information such as social security numbers, balances in checking accounts, credit card information, healthcare information, and other private data is solved by the GDPR and the California Consumer Privacy Act is solved and everyone is satisfied; not exactly. However, the U.S. and the world legal and business communities are evolving much like the U.S. developed after enacting the constitution. Society clearly saw a need and the legal system has begun to provide standards for businesses and consumers to follow. Eventually, on a case by case basis, the legal system will provide the framework for all to benefit. This is good for business having a set of defined rules to follow and good for the consumer. Once we know the standards, the reasoning of stare decisis does the rest. Meaning, the legal decisions that have been made must be followed providing fairness and consistency in society.

Clearly, society benefits from clear consistent decisions from the judicial branch of government.

> In Portia's words, a single wrong decision need only be recorded for a precedent, and many an error by the same example will rush into the state. Of course, in practice stare decisis probably is not often as bad as all that. Just as it can institutionalize erroneous results, it also can (and certainly often does) ensure that just decisions are reproduced more often than they otherwise would be. And the rule of stare decisis as currently observed in Anglo-American law is not a strict one: Courts can decline to follow their own previous decisions when those precedents are judged to be clearly in error. Lawyers and judges, moreover, regularly display amazing ingenuity in "distinguishing" unfavorable precedents that otherwise would be "controlling". In the real world, then, the prospect of grievous injustice "rushing into the state" may seem rather remote. But the prospect exists nonetheless. Courts may be adept at manipulating precedent to reach decisions they want to reach, but they are not always able or willing to do so; sometimes courts believe (or claim to believe) they are bound by stare decisis to reach results they think unjust. (Peters, 1996, p. 2034)

If the doctrine of stare decisis is a flawed principle, eventually, businesses will put in place business polices that are consistent with the law. The point is that businesses make the difference. It is up to business to take action if we have any hope of success. In order to do so, a skillful management needs to explore and be mindful of legal risk and liability. Vague laws and inconsistent legal decisions make it more difficult to operate a corporation. Something is better than nothing.

Clearly the GDPR and the California Consumer Protection Code are a major step to help

> to reduce the risk of pursuing the wrong opportunity. The process of creating the business plan helps to minimize opportunity costs. Writing the business plan helps you assess the attractiveness of this particular opportunity, versus other opportunities. To plot your course and focus your efforts. The business plan provides a roadmap from which to operate, and to look to for direction in times of doubt. Without a business plan, you may shift your short-term strategies constantly without a view to your long-term milestones. To reposition your business to deal with changing conditions. For example, during difficult economic conditions, if your current sales and operational models are not working, you can rewrite your business plan to define, try, and validate new ideas and strategies. (Lavinsky, 2020)

Ultimately, it is up to business to translate the law into viable corporate practices that are followed and make a difference. The law in and of itself will not do anything. It is a challenge. Businesses will develop their plans.

In addition to the aforementioned regarding the GDPR and the CCPA, there is one more source of authority to consider for international and domestic corporations doing business in the U.S. In order to assess compliance, one must get all of the standards. That includes the Federal Trade Commission decisions on data breaches. The Federal Trade Commission (FTC) is the federal regulatory legal adjudicator of data security breach matters. When a data breach occurs, consumers may file a complaint with the FTC. The FTC rulings and regulations apply to all corporations doing business in the U.S. unlike the GDPR which applies to corporations doing business in Europe and the CCPA for corporations doing business in California. The FTC then decides the matter and the decision becomes precedent setting and must be followed. A good example of an FTC ruling is in the landmark ruling in the Card Systems case. In this case, a credit card bank was hacked resulting in the exposure of private information regarding the customers of the bank. The ruling is important because the FTC set important legal parameters that set the stage for a negligence cause of action in the federal courts. It is a well-established principle that when one violates a statute, ruling, or regulation, it creates a presumption of the breach of the reasonable duty of care, one of the first elements of a negligence cause of action. In other words, if one violates the speed limit, and has an accident, there is a presumption that the driver of the car was negligent. This very principle makes this FTC ruling defining and important. In the Card Systems case, the FTC ruled the following:

> In processing transactions, Card Systems collected card numbers, expiration dates and other information, and the data was stored on its computer network. The FTC accused Card Systems of failing to have enough security measures in place to keep hackers out of its computer network and to limit access between computers on its network and between its computers and the Internet. Among other things, the company did not do enough to detect or investigate unauthorized access to personal information, the agency said. The lack of security compromised millions of credit and debit cards and led to millions of dollars in fraudulent purchases, the FTC said. The FTC said it would publish the proposed settlement in the Federal Register and then accept public comments for 30 days before finalizing the settlement. Pay by Touch acquired Card Systems in January 2006, said a company spokeswoman in an e-mail response. In the past several months, the former Card Systems has passed audits conducted by highly regarded independent security experts following extensive investments to improve its security program. (Reuters, 2006)

From the preceding case, it is clear that the FTC means business because the ruling states that the bank did not do enough to find out what went wrong when the data breach occurred. Millions of people were affected by this data breach because much of the personal information associated with credit card applications including personal credit card numbers was stolen. Now we definitely know that companies must keep data secure and investigate any breaches. If companies do not perform their due diligence, they are in violation of federal law.

Putting the GDPR and the CCPA and the FTC together is great onus of compliance. This increases the responsibility for corporations to pay attention to computer cyber security, domestically and at the international level. The rulings are good for corporations because the laws and the rulings provide a set of principles intended for corporations to set up the best management practices regarding data protection. With this knowledge, if followed, corporations have a good defense against data breach liability claims. Good for society, good for business.

Businesses no longer have to guarantee protection. On the side of business if the law is followed, and business has complied with the law, corporations may introduce the mounds of evidence of the actions and protections undertaken to protect data and mitigate liability. In addition, not all breaches make it through the rigor of a lawsuit to damages. Proving actual, sustained, in fact damages is a big problem for the consumer whose privacy has been breached. Early litigated cases point to the damages proof problem; there is still a lot of trouble establishing both causation and damages. In other words, if cybersecurity systems are breached, courts are reluctant to find actual damages other than mere inconvenience. Mere inconvenience, in the courts usually is not enough damages to compensate and pay plaintiffs for litigation. Plaintiffs must pay attorneys upfront expenses/fees, and this is a huge deterrent for many litigants. At the end of a majority of the cases, results are mixed. This is a big break for domestic and international corporations.

Take this example,

> Not all plaintiffs have been unsuccessful. In Bell v. Michigan Council 25 the plaintiffs were members of the defendant union. The treasurer of the union took the plaintiffs' personal information home. The treasurer's daughter was later convicted of identity fraud after a notebook was found in her possession listing the names, social security numbers and drivers' license numbers of the plaintiffs as well as the fraudulent purchases made in their names. The plaintiffs succeeded in their arguments that the union owed them a duty to protect their personal data against misuse by third parties, that the union had been careless in failing to protect their personal data, and that this negligence had facilitated the identity theft. (Chandler, 2007)

For domestic and international business, this means more cost, risk management and potential liability and the need for good legal advice.

> This means identifying and addressing the risks that are likely to arise based on the nature of their business, the places where they conduct business and the customers they serve. It also means evaluating the degree to which foreign parties—whether subsidiaries, joint ventures or even contractors—engage in activities that expose their U.S. counterparts to civil and criminal liability. By taking a comprehensive approach, companies can best manage their risk and mitigate costs by conducting periodic risk assessments, crafting tailored internal controls, conducting frequent training and coordinating common standards across their entire organizations. (Husisian, 2018)

This does bring us to the current conditions involving the impact of the Corona Virus upon cybersecurity systems. Businesses here and abroad are having a tough time generating top line revenue growth. In fact, many firms can no longer afford the luxury of developing competent cyber security systems. The situation out there is bleak.

> Even before the virus, the security paradigm was changing. The network perimeter was already dissolving, and now it's completely dissolved, Buffomante said. Some organizations wrongly assume that by moving to the cloud, they're outsourcing security. In reality, cloud security is a shared responsibility, Buffomante said. To protect themselves, companies must correctly configure firewall connections and align data access with their internal security policies, instead of going with the default of unlimited access to corporate data. They should also monitor for suspicious activity, so that if someone logs in from Chicago and tries again from Singapore an hour later, their identity can be verified or their access shut off before a breach occurs. (Meek, 2020)

At the very least, many corporations currently have the systems in place that existed before the virus. It is my perception that if you were a corporation that followed the law and had good cyberwatch systems before the virus and you are currently doing the same thing, you probably have enough policies and procedures in effect to meet the due diligence requirements reducing risk of liability.

Conclusions and Recommendations

1. If you are a corporation doing business in California, follow the CCPA. By following the CCPA you are likely going to be within the FTC federal guidelines because the corporation is following the law and is therefore not negligent.

2. If you are outside of the subject matter jurisdictional limit of the CCPA, follow the FTC rulings and regulations. The FTC rulings and regulations are the law of the land in the U.S. All corporations doing business must meet the minimum requirements of the FTC rulings and regulations. Following the GDPR is secondary authority. However, the GDPR is so exact and comprehensive that a corporation following the GDPR may well be within the due diligence requirements of the FTC. This explains why many multi-national corporations get cybersecurity audits where the auditors follow the GDPR even if the corporation files accounting reports on risk assessments to the authorities in the U.S.

3. Following the law is a defense to any action in negligence. Coupled with the difficulty proving causation and damages, if a corporation can provide a mountain of evidence that it did all that it could to comply with the FTC rulings and regulations, the CCPA if doing business in California and the GDPR, this substantially reduces if it not eliminates concerns of liability from lawsuits.

4. If a corporation is doing business in Europe, it must comply with the GDPR. The GDPR is a good model for California and other states in the U.S. to follow. The GDPR may also be helpful to the FTC in crafting more specific rulings. If doing business in the U.S. only, the GDPR is only secondary persuasive authority. Meaning, any legal adjudicatory body in the U.S. is not mandated to follow the GDPR; it is only suggested. When there are no other standards to follow in the U.S., corporations do find good reason to establish the due diligence standard within the corporation by following the GDPR. Further, if you are in international firm doing business in the U.S., the element of internet cyber jurisdiction could present problems for those who may be subject to the laws of states much to their surprise. Much is still left to interpretation no matter how you view it.

5. Finally, within the provisions of any legal system, if you are an international firm doing business in the U.S. or a U.S. firm doing business in Europe, within the U.S. legal system and the GDPR jurisdictions, if a firm remains proactive, current, and systematic about protecting data, and notice to consumers is appropriate in the case of data breaches so consumers have an opportunity to protect themselves, you will be legally sound and probably will only have to deal with the problem from a business perspective. Legally, your work in cybersecurity must be reasonable involving the latest technology to protect data and your proactive nature

should be enough to mitigate the damage if not completely exonerate you in a lawsuit. The best protection is to have an outside cybersecurity firm and their legal experts assess your systems, to make recommendations for you to follow with ongoing reviews. It is worth your time, effort, and investment.

References

Chandler, J. (July 20, 2007). Negligence liability for breaches of data security. *SSRN.* Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=998305 (Last visited June 28, 2020)

Fertik, M. (January 27, 2020). CCPA is a win for consumers, but businesses must now step up on CX. *Forbes.com.* Retrieved from https://www.forbes.com/sites/michaelfertik/2020/01/27/ccpa-is-a-win-for-consumers-but-businesses-must-now-step-up-on-cx/#71b9fd096557 (Last visited June 24, 2020)

Fimin, M. (March 29, 2018). Five benefits GDPR compliance will bring to your business. *Forbes.com.* Retrieved from https://www.forbes.com/sites/forbestechcouncil/2018/03/29/five-benefits-gdpr-compliance-will-bring-to-your-business/#6fb0ed67482 (Last visited June 25, 2020)

Husisian, G. (2018). Know the risks: Domestic and international compliance. Retrieved from https://www.foley.com/en/insights/publications/2018/03/know-the-risks-domestic-and-international-compliance (Last visited July 21, 2020)

Lavinsky, D. (2020). 20 reasons why you need a business plan. *Growthink.com.* Retrieved from https://www.growthink.com/content/20-reasons-why-you-need-business-plan (Last visited June 27, 2020)

Meek, T. (June 11, 2020). The CIO factor. Retrieved from https://www.cio.com/article/3562417/restarting-america-reengineering-cybersecurity-for-the-new-reality.html (Last visited July 21, 2020)

Peters, C. J. (1996). Foolish consistency: On equality, integrity, and justice in stare decisis. *The Yale Law Journal, 105*, 2031-2035. Retrieved from https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=7699&context=ylj

Reuters. (2006). FTC settles with Card Systems over data breach. Company must adopt security measures, undergo audits. Retrieved from https://www.computerworld.com/article/2562978/ftc-settles-with-cardsystems-over-data-breach.html (Last visited June 27, 2020)

Sabastian, F. (June 21, 2019). GDPR in the U.S.: Requirements for U.S. companies. *Termly.io.* Retrieved from https://termly.io/resources/articles/gdpr-in-the-us/ (Last visited June 25, 2020)

Sirota, D. (November 14, 2019). Extra Crunch: California's new data privacy law brings U.S. closer to GDPR. The requirements aren't insignificant, and the fines could add up. Retrieved from https://techcrunch.com/2019/11/14/californias-new-data-privacy-law-brings-u-s-closer-to-gdpr/ (Last visited June 28, 2020)