The New Age Of Cybersecurity
Privacy, Criminal Procedure And
Cyber Corporate Ethics

Paul J. Morrow, Husson University, USA
Stephanie Shayne, Husson, University, USA

ABSTRACT

This paper reviews cybersecurity and the new criminal procedure standards of searches and seizures based on the perspectives of probable cause in the digital age involving cell phones. Also, this paper examines the civil corporate policy perspectives involving data breaches as the topic relates to the consumer using social media and provides guidance for executives to enact proper and responsible corporate policies navigating the new cybersecurity landscape in the post - Carpenter vs. U.S. era.

Reading this paper is worth your time because: (1) you will learn the new cybercrimes legal standards involved with cyber-privacy and the criminal process which is necessary to develop director competencies; (2) you will gain knowledge which is the key to proposing ethical systems within the corporation required by law; (3) moving forward, we are at a critical point in America and good guidance is vitally important.

Keywords: Cybersecurity; Criminal Procedure; Searches and Seizures; Probable Cause; Cell Phones; Data Breaches; Corporate Policy; Social Media

INTRODUCTION

The U.S. Supreme Court in Carpenter v. U.S. surgically examines the legal boundaries of the procurement of cell phone data by the government and issued a blockbuster decision in July of 2018 that profoundly affects ferreting out of cybercrimes and business decisions involving corporate cybersecurity. Before Carpenter v. U.S. if you shared information with third parties, there was no reasonable expectation of privacy in the shared data. The government had free discovery privileges to the cell phone records. Now, that is all changed. The U.S. Supreme Court ruled in U.S. vs. Carpenter that the government must have probable cause to search the cellphone of a criminal suspect. This decision has far-reaching implications for executives. Operating in a global economy doing business in the U. S., the directors of a corporations need advice regarding the global cyber technological legal aspects of cybersecurity or risk being liable for not having enough legal knowledge to avoid criminal or reckless corporate decisions. In addition to the courts, Congress continues to plead with the Chief Executive Officers of multinational corporations who testify to cyber legal issues and management issues affecting civil cases. For example, in light of the issues at Facebook, it is abundantly clear that there is a serious gap in what directors of corporations, small business owners, and consumers do not know. The need for an introspection and research is great.

“It’s why experts say it’s so crucial to train everyone in the company on cyber security, from the front desk person to the CEO, rather than just delegate the issue to a select few in the IT. In the past five years, the U.S. Attorney’s Office in San Diego prosecuted eight computer hacking cases and at least 14 involving the theft of credit card or banking data, according to the office. The number of cyber prosecutions is likely low because cyber-crimes often get charged under other various laws, including wire fraud, Feve said. Cyber cases also bring unique challenges to the courtroom. Digital evidence might be overseas. Hackers may delete or encrypt evidence. And lawyers need technical expertise to make a jury understand complex evidence and processes, Feve said. National security investigations, those can take years and years, and often remain top secret. Attribution in cyber (crime) is extremely difficult, and criminals realize that. It’s low risk and potential high reward for cyber criminals, said Stephen Cobb, a security researcher at ESET, one of the world’s largest security software firms. It’s hard to fight back if you don’t know for sure who carried out the attack and why.
This past year saw a number of massive breaches that remain under investigation and highlight the growing threat. 

To act responsibly, the courts and law makers in both criminal and civil cases need to continue to pursue avenues of knowledge to make proper legal and ethical decisions without leaving huge gaps in reasoning. The internet also affects children and schools which does compound the problems. Our current efforts are noble. More must be done addressing the practical nuances left open by Carpenter v. U.S. and other civil corporate policy nuances.

Given the complexities in the realm of cybercrime, it is important to examine the issue from a number of perspectives. This paper first looks at the evolution of criminal procedure as it pertains to the constitutionality of obtaining cell phone and other data. The paper then considers the issue in the context of civil litigation and corporate ethics.

THE CONSTITUTIONAL CRIMINAL PROCEDURE OF CYBERSECURITY

“Cell phones perform their wide and growing variety of functions by continuously connecting to a set of radio antennas called cell sites. Each time a phone connects to a cell site, it generates a time-stamped record known as cell-site location information (CSLI). Wireless carriers collect and store this information for their own business purposes. Here, after the FBI identified the cell phone numbers of several robbery suspects, prosecutors were granted court orders to obtain the suspects’ cell phone records under the Stored Communications Act. Wireless carriers produced CSLI for petitioner Timothy Carpenter’s phone, and the Government was able to obtain 12,898 location points cataloging Carpenter’s movements over 127 days—an average of 101 data points per day. Carpenter moved to suppress the data, arguing that the Government’s seizure of the records without obtaining a warrant supported by probable cause violated the Fourth Amendment.”

The analysis begins with the constitutional authority to search without a warrant.

“Because the Fourth Amendment protects people, rather than places, its reach cannot turn on the presence or absence of a physical intrusion into any given enclosure. The "trespass" doctrine of Olmstead v. United States, 277 U. S. 438, and Goldman v. United States, 316 U. S. 129, is no longer controlling. Pp. 389 U. S. 351, 389 U. S. 353.”

From this decision, electronic signals fall within the ambit of the 4th amendment of the Constitution. This leads us to the legal authority of the government to conduct criminal investigations.

The standard for criminal investigation is illustrated in Terry v. Ohio 392 U.S. 1 (1968) where the U.S. Supreme Court states:

“For this purpose it is urged that distinctions should be made between a ‘stop’ and an ‘arrest’ (or a ‘seizure’ of a person), and between a ‘frisk’ and a ‘search.’ Thus, it is argued, the police should be allowed to ‘stop’ a person and detain him briefly for questioning upon suspicion that he may be connected with criminal activity. Upon suspicion that the person may be armed, the police should have the power to ‘frisk’ him for weapons.”

This further leads us to searches but with probable cause.

“Probable cause exists where "the facts and circumstances within their [the officers'] knowledge and of which they had reasonably trustworthy information [are] sufficient in themselves to warrant a man of reasonable caution in the belief that an offense has been or is being committed.” Brinegar v. United States, 338 U.S. 160 (1949) citing: Carroll v. United States, 267 U. S. 132, 162 “These long-prevailing standards seek to safeguard citizens from rash and unreasonable interferences with privacy and from unfounded
charges of crime. They also seek to give fair leeway for enforcing the law in the community's protection. Because many situations which confront officers in the course of executing their duties are more or less ambiguous, room must be allowed for some mistakes on their part. But the mistakes must be those of reasonable men, acting on facts leading sensibly to their conclusions of probability.”

Do any of these precedents apply to searching telecommunications records without a warrant?

The U.S. Supreme Court ruled in U.S. v. Carpenter that the government must have probable cause to search the cellphone of a criminal suspect. Now, the government needs a search warrant issued by a judge increasing objectivity, particularity, and reasonableness. The reasons why are as follows:

“The digital data at issue—personal location information maintained by a third party—does not fit neatly under existing precedents but lies at the intersection of two lines of cases. One set addresses a person’s expectation of privacy in his physical location and movements. See, e.g., United States v. Jones, 565 U. S. 400 (five Justices concluding that privacy concerns would be raised by GPS tracking). The other addresses a person’s expectation of privacy in information voluntarily turned over to third parties. See United States v. Miller, 425 U. S. 435 (no expectation of privacy in financial records held by a bank), and Smith, 442 U. S. 735 (no expectation of privacy in records of dialed telephone numbers conveyed to telephone company).”

Historically, the whole purpose of the 4th amendment pertains to,

“the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.”

The “basic purpose of this Amendment,” our cases have recognized,

“is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials.” Carpenter v. U.S. citing Camara v. Municipal Court of City and County of San Francisco, 387 U. S. 523, 528.

On this score, our cases have recognized some basic guideposts. First, that the Amendment seeks to secure “the privacies of life” against “arbitrary power. Carpenter v. U.S. 2018 WL 3073916 (2018) citing Boyd v. United States, 116 U. S. 616, 630 (1886). Second, and relatedly, that a central aim of the Framers was,

“to place obstacles in the way of a too permeating police surveillance. citing United States v. Di Re, 332 U. S. 581, 595 (1948).”

"Based on that information, the prosecutors applied for court orders under the Stored Communications Act to obtain cell phone records for petitioner Timothy Carpenter and several other suspects. That statute, as amended in 1994, permits the Government to compel the disclosure of certain telecommunications records when it “offers specific and articulable facts showing that there are reasonable grounds to believe” that the records sought “are relevant and material to an ongoing criminal investigation.” 18 U. S. C. §2703(d).”

The basis of the governments search is a statute. The U.S. Supreme Court nullifies the search as unconstitutional and states the following:

“Having found that the acquisition of Carpenter’s CSLI was a search, we also conclude that the Government must generally obtain a warrant supported by probable cause before acquiring such records. Although the “ultimate measure of the constitutionality of a governmental search is ‘reasonableness,’ ” our cases establish that warrantless searches are typically unreasonable where “a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing.” Vernonia School Dist. 47J v. Acton, 515 U. S. 646, 652–653 (1995).

5 Brinegar v. United States, 338 U.S. 160 (1949)
6 Carpenter v. U.S. 2018 WL 3073916 (2018)
7 Id
8 Carpenter v. U.S. 2018 WL 3073916 (2018)
Thus, "in the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement." citing Riley, 573 U. S., at __ (slip op., at 5).

The Government acquired the cell-site records pursuant to a court order issued under the Stored Communications Act, which required the Government to show "reasonable grounds" for believing that the records were "relevant and material to an ongoing investigation." 18 U. S. C. §2703(d).

That showing falls well short of the probable cause required for a warrant. The Court usually requires, "some quantum of individualized suspicion" before a search or seizure may take place. United States v. Martinez-Fuerte, 428 U. S. 543, 560–561 (1976).

"Under the standard in the Stored Communications Act, however, law enforcement need only show that the cell-site evidence might be pertinent to an ongoing investigation—a "gigantic" departure from the probable cause rule, as the Government explained below. App. 34. Consequently, an order issued under Section 2703(d) of the Act is not a permissible mechanism for accessing historical cell-site records. Before compelling a wireless carrier to turn over a subscriber's CSLI, the Government's obligation is a familiar one—get a warrant." 9

By the aforementioned language, the U.S. Supreme Court ushered criminal investigations into the digital age requiring a search warrant to search cell phone records. So, if one is a corporate executive and the government is investigating a white-collar crime, the government must obtain a search warrant to search your cell phone records absent exigent circumstances.

One notable exception to the warrant requirement that is still applicable is when the government must hurry to gather the evidence based on the safety of the officer or that there is an immediate risk of the destruction of the evidence. This exception is not so likely to apply to cell phone records because the threat is not immediate. The court addressed the issue of exigent circumstances to the warrant requirement of the 4th amendment by stating the following:

"Further, even though the Government will generally need a warrant to access CSLI, case-specific exceptions may support a warrantless search of an individual's cell-site records under certain circumstances. "One well-recognized exception applies when "the exigencies of the situation" make the needs of law enforcement so compelling that [a] warrantless search is objectively reasonable under the Fourth Amendment." Kentucky v. King, 563 U.S. 452, 460, 131 S.Ct. 1849, 179 L.Ed.2d 865 (2011) (quoting Mincey v. Arizona, 437 U.S. 385, 394, 98 S.Ct. 2408, 57 L.Ed.2d 290 (1978)). Such exigencies include the need to pursue a fleeing suspect, prevent individuals who are threatened with imminent harm, or prevent the imminent destruction of evidence. 563 U.S., at 460, and n. 3, 131 S.Ct. 1849. As a result, if law enforcement is confronted with an urgent situation, such fact-specific threats will likely justify the warrantless collection of CSLI. Lower courts, for instance, have approved warrantless searches related to bomb threats, active shootings, and child abductions. Our decision today does not call into doubt warrantless access to CSLI in such circumstances. While police must get a warrant when collecting CSLI to assist in the mine-run criminal investigation, the rule we set forth does not limit their ability to respond to an ongoing emergency."10

So here the Supreme Court left open the notion that if the threat of the destruction of the evidence is immediate and there is no time to obtain a warrant, the government may proceed without a warrant. This rule has been around for quite some time. It gives the government an opportunity to protect the officer and the evidence and is still good law.

Noticeable is the gap between probability and reasonable articulable suspicion especially in discovery of cell phone data held by third parties. Also, probability in many instances is a quantifiable statistical scientific term. In science, data must be generated for objectivity and based on the sample population of the data of a specific subject. In business,
the probability of achieving certain investment returns are based on sales and cost of production. Both science and business rely upon real data numbers for the basis of a decision using mathematical equations.

Thus, is not the case in the determination of probable cause in criminal cases. The need for an independent magistrate to rule on whether or not certain probabilities exist in many instances is based on the perceptions of the government that probable cause exists that a certain crime has been committed. In addition to the lack of objectivity argument, crimes usually involve some sort of intent. It is well established that the concurrence of intentional commitments to commit a crime and the act of committing the crime must converge. Intention is defined as “conscious object”. In other words, a defendant in most cases must have the conscious object of committing a specific crime to determine whether there is probable cause that a crime has been committed. Again, the existence of probable cause that the defendant intended a crime is based on officer perception with no assistance from the profession of psychology.

So, other than the officer’s perception, we were left with the constitutional boundary of determining probable cause in cyber cases to: 1. the lack of data determination and 2. no psychological expert to determine intentionality. Arguably, the current process leads to unscientific conclusions for searching anything that we own, including our homes as a constitutional standard to determine probable cause. The same problem exists with the standard for criminal investigations involving reasonable articulable suspicion that criminal activity is afoot under Terry v. Ohio. Investigations criminal or civil may be based on the vagaries of perception and lack of objectivity creating a veil of suspicion and an aura of doubt that affects how we live and work. Now, that has all changed and the U.S. Supreme Court certainly sent a strong message protecting the right to privacy by requiring search warrants for the discovery of cell phone data tilting the scales toward objectivity and impartiality ushering in the digital age of discovery. A decision by the U.S. Supreme Court that illustrates the new era of American constitutionalism. Many feel it was the right move.

CONCLUSIONS

Our founding fathers envisioned objectivity and particularity in making these decisions and due process requires it. Digital data is susceptible to the dumping of information during general swathe searches with tons of irrelevant data private to the general population. The areas of potential improvement are as follows:

1. It might help if cases are referred to grand juries for verification before a warrants issue. In some very serious cases, there is not time. The criminal must be caught. In many cases involving substantial, corroborated evidence, there is time. In the corporate setting, white collar crimes involve extensive investigations and there is time.
2. In balancing the need to ferret out crime, verses invasiveness, decisions may be based on perception rather than verifiable data and scientific judgment. Prosecutors put themselves at risk of losing cases on motions to suppress if a warrant is not procured.
3. Congress could pass legislation to address the nuances incorporating U.S. v. Carpenter. For example, it has been done in the past in the civil rights area.
4. The right to be who you want to be without being monitored really matters in our society because it affects motivation, achievement and a fundamental need of being free. We must continue to educate people of all walks of society and people who run corporations. Teach the arguments on the issues from both sides.
5. Take technology from this point and move forward. There is no need to get bogged down in the decisions of the past that have now been modified. Let’s move onward to the civil corporate side.
6. It is simple. Where there is a lack of exigency, require a warrant to maintain objectivity, obtain the best evidence possible with an eye towards preserving the privacy of the citizens. This is the new standard.

THE CORPORATE CIVIL LITIGATION PERSPECTIVE

The civil corporate side of the equation is quite different than the criminal procedure perspective although criminal procedure would apply to the discovery of the evidence on a cellphone if the Federal Trade Commission and/or the Securities and Exchange (the government) initiated proceedings against a corporation seeking evidence from executive text messages and cellphone discussions. “Facebook has confirmed that the FBI, SEC, and FTC have all joined the Justice Department in asking questions about user data being improperly shared with political consulting firm Cambridge Analytica. Facebook could not confirm whether the agencies are coordinating their efforts. The stock slipped roughly 1.5 percent after-hours on Monday after The Washington Post first reported that federal investigators
were broadening their inquiries into the company's data sharing practices. The stock closed down 2.35 percent on Tuesday as trading ended early for the Independence Day holiday.\(^{[11]}\)

Criminal procedure is more concerned with the government discovering the evidence in criminal cases to convict and punish the executives of a corporation. Civil litigation is more concerned with money damages or injunctive relief. Such is the case with Facebook currently in front of the both the SEC and the FTC for the violation of an FTC consent decree to inform consumers of the sale of their data to a firm, Cambridge Analytica. Also, at issue are the implications of violating SEC rules by Facebook for its duty to disclose to investors the selling of private data to the same Cambridge Analytica which is now bankrupt. Shareholders of Facebook have reasonable grounds against Facebook in negligence for the drop-in market value of the stock price. “The scandal has caused Facebook to delay the unveiling of new home products and redesign its privacy settings. The stock has lost almost $100 billion in market value and is no longer among the top five most valuable companies in the world. The shares closed up 0.53 percent Wednesday at $153.03.”\(^{[12]}\) The price of Facebook stock dropped substantially in July 2018.

We all know that the sharing of data from all platforms, and not just social media has become a serious problem in our time. “For many companies, sharing cybersecurity information with public and private partners should be part of a comprehensive cybersecurity program. By sharing, companies broaden the pool of information that the government and other companies can use to defend against attacks, which resounds to everyone’s benefit. Although CISA likely does not fundamentally change the cybersecurity landscape, it does tip the scale toward greater information sharing by offering limited protections and creating more certainty as to how, why, and why not to share cyber threat and defensive measure information.”\(^{[13]}\)

Society is at a loss for prescribing methods that help companies become more responsible. Several recommendations have been put forth to hold tech companies to higher levels of accountability. These measures include: (1) imposing fines for data breaches, (2) policing political advertising and are best exemplified as follows:

> “The four ways to make tech companies more responsible are “Impose fines for data breaches..., police political advertising..., make tech companies liable for objectionable content..., and install ethics review boards.

> *Imposing fine is punitive and does affect the internal decision making within the corporation. If the board of directors of a corporation learns that millions of dollars in fines have been imposed by the Federal Trade Commission, it is their duty to investigate and not let it happen again.”*\(^{[14]}\)

The idea of policing content is much more difficult because of the first amendment issues. It is a good idea to rule out the extremely threatening material in a particular domain. The first amendment does not protect all expression especially when children are affected. There are exceptions to first amendment protections and companies must be aggressive to get those messages out of their domains. Many social media companies cater to kids 5 to 13 years of age.

The notion of civil liability for objectionable content is a good jurisprudential idea. These safeguards are founded in civil litigation. In other words, the act of bringing an action against a company for trademark, copyright and intellectual property rights violations makes directors, clients, investors and consumers take notice. This all adds to transparency and is good. Amazon in now facing scrutiny because of the potential sharing of its list of purchasers. Corporations should be responsible to more than just the shareholders.

Finally, installing ethics review boards is probably the best of all of the ideas. Companies like Facebook and Amazon would benefit greatly. Establishing review boards inside the company and outside the company invoking objectivity,

\(^{[11]}\) D’Onfro, J. (July, 2018). Facebook confirms that SEC, FBI, and FTC have asked questions about Cambridge Analytica. Retrieved from: https://www.cnbc.com/jillian-donfro/ (Last visited July 9, 2018)

\(^{[12]}\) Bloomberg. (2018, March) Facebook may have breached a 2011 consent agreement, FTC says. Retrieved from: http://fortune.com/2018/03/29/cambridge-analytica-facebook-scandal/ (Last visited July 9, 2018)

\(^{[13]}\) Brad, S. Karp, Paul, Weiss, Rifkind, Wharton & Garrison LLP, (2016). Comments off on Federal guidance on the Cybersecurity Information Sharing Act of 2015. Retrieved from: https://corpgov.law.harvard.edu/2016/03/03/federal-guidance-on-the-cybersecurity-information-sharing-act-of-2015/. (Last visited July 9, 2018)

\(^{[14]}\) Angwin, J. (2018) Four ways to fix Facebook. Retrieved from: http://business-ethics.com/2018/04/08/four-ways-to-fix-facebook/ (Last visited: July 19, 2018)
allows people to resolve their differences through a mediation process with experts from many disciplines. Most of all, the review board process is akin to the way society functions best. It allows all sides of an argument to be presented and to fashion a response that fits all of the stakeholders involving many experts saving time and money. The process is quicker, less formal and more productive. Many professional boards like the Bar Association for attorneys have overseers for the purposes of legal ethics compliance and they do a great job.

INTERNATIONAL IMPLICATIONS AND LEGAL CONCERNS

Given both the criminal and civil implications of the government’s right to search the cell phone of an executive, we must now consider the implications for executives in the international corporate sector. If you are a corporation based out of another country doing business in the U.S., you are subject to the laws of the U.S. In many countries where there are businesses stationed here in the U.S., the expectation of privacy may be very different.

The implications for the corporate sector and the legal jurisdictional limitations are global.

“...Cambridge Analytica may be an issue not only for Americans and Britons. The firm claims to have worked in a wide range of countries, including Australia, Brazil, Kenya, Malaysia and Mexico. Politicians in several of those countries are calling for investigations of the company’s work and local partners are distancing themselves.”

Foreign companies need to be educated about our constitution and its protections. For example,

“In order for a case to be properly heard, a court must have personal jurisdiction over the parties. If a court is found to not have jurisdiction on appeal, a verdict can be overturned which is a disaster. This can cost millions of dollars in time and effort litigating a case only to find that the court in which the case was heard did not have the authority to decide the case from the beginning. As one can imagine, it is a popular litigation strategy to contest jurisdiction on appeal because of its summary way to dispose of a case altogether.”

In many countries there is no governing constitution limiting police discretion. For international corporations, the constitution of the U.S. changes the landscape substantially. Subject matter jurisdiction in the U.S. does become an issue. For example,

“When the agency itself brings the action, it is usually for the public good or on behalf of society. The impact of the wrongful conduct is so great that the government agency must stop the activity. The legal significance of the a party getting a decision from the administrative agency, deemed by the courts as a specialist in the field, is that the decision may be binding on the court action filed by the Plaintiff. So, in a cyber-attack liability case, it is to the advantage of the plaintiff, whether it is the government or private parties, to secure an administrative agency decision. Also, the administrative agency conducts its own fact finding, and provides a quicker more inexpensive snap-shot of the factual legal merits of a case. One issue that is heavily contested is whether the administrative agency had jurisdiction, or authority to decide the case in the first place. If not, then the case gets dismissed usually with no repercussions. The case filed in court now has to proceed on its own merits without the benefit of a favorable decision by the administrative agency. Court cases take a long time and are extremely expensive. Receiving an unfavorable determination from the administrative agency is usually a fatal blow the case filed in court. FTC jurisdiction in cyberattack cases is monumental.”

Also, multiculturalism definitely comes into play. The business model in other countries may be very different than the business model in the U.S. Simply doing what may be legally correct is required but may not be enough to stay in business. Values and culture affect business decisions and profits.

15 Taylor, Adam, (2018). Cambridge Analytica’s reach went far beyond the U.S. elections. Retrieved from: https://www.washingtonpost.com/news/worldviews/wp/2018/03/20/cambridge-analyticas-reach-went-far-beyond-the-u-s-elections/?noredirect=on&utm_term=.a649e735a58c (Last visited, July 9, 2018)

16 Morrow, P (2017). Assessing multinational global cyber business risk of cyberattacks –Minimizing the risk of loss due to wrongful jurisdiction Retrieved from: https://www.cluteinstitute.com/ojs/index.php/JCR/article/view/9961/10062 (Last visited July 18, 2017)

17 Id.
In other words, compliance with the law may not be an effective measure to achieve true multinationalism. In the context of international joint ventures, in addition to compliance with the law there are cultural concerns in practice affecting relationships, particularly when corporations come from underdeveloped countries. What is being allowed in China or other countries may be very different from the way we operate in the U.S. Therefore, the foreign corporation’s business model must be adapted and adjusted to be successful in the U.S. It means, more challenges to resolve and makes doing business in the U.S. much more difficult. Foreign investors are adapting quickly. The law is way behind the technology. It is up to the directors of a corporation to define their corporate responsibilities regarding social media. It does become a matter of business ethics.

THE BUSINESS ETHICS PERSPECTIVE IN THE U.S. AND GLOBALLY

There are many concerns with ethics and technology in the U.S. and globally. More cooperation is necessary. Major questions about deterrence exist as well. The global companies like Facebook have a lot of cash. A fine, may not be punishment enough for the company and its executives. A case in point is the fact that Facebook is in current violation of the consent decree. Obviously, this is a business ethics issue for Facebook. Despite the fact that it is a well-run company, measured by the demand for its product and the price of the stock, Facebook must initiate procedures to protect the privacy of its customers, ethically.

“Facebook said it would roll out a centralized system for its users to control their privacy and security settings in response to an outcry over the way it has handled personal data. The system, which will be introduced to Facebook users globally over the coming weeks, will allow people to change their privacy and security settings from one place rather than having to go to roughly 20 separate sections across the social media platform. From the new page, users can control the personal information the social network keeps on them, such as their political preferences or interests, and download and review a file of data Facebook has collected about them. Facebook also will clarify what types of apps people are currently using and what permissions those apps have to gather their information” 18

It still leaves the question of exactly what is being done in the company and its culture.

A lot remains to be seen regarding the new procedures. On both the civil and criminal side, the response of the corporation is to initiate corporate audits to reduce the risk of cyberattacks and violations of the right to privacy of sharing information. All of this compounded by the use of Facebook by children.

“While Facebook is claiming the data they are collecting about kids in this app won’t be used for advertising, it doesn’t promise not to use the data to build profiles on our kids and their families that will later be utilized against them in the future by insurance companies, employers, colleges, law enforcement, governments, etc.” 19

In addition, the risk of sharing information, all of the other problems and more do exist. For example, corporations struggle every day with

“the tests included simulating more than 2,000 separate incidents: denial of service attacks, website defacements, access to sensitive information and attacks on critical infrastructure. Software and hardware failures were judged the biggest security threats.” 20

This costs so much money and although many foreign corporations have done some work, a lot more needs to be done.

18 Frenkel, S. and Singer, N. (2018, March). Facebook Introduces Central Page for Privacy and Security Settings. Retrieved from https://www.nytimes.com/2018/03/28/technology/facebook-privacy-security-settings.html (Last visited July 9, 2018)
19 Shear, B (2017, December). Avoid Facebook’s New Messenger App for Kids to Protect Your Family’s Privacy and Future. Retrieved from: https://www.studentprivacymatters.org/avoid-facebookss-new-messenger-app-for-kids-to-protect-your-families-privacy-future/ (Last visited, July 9, 2018)
20 Gabel, D. L. Bertrand D. Orzechowski (2015, July). Cyber risk: Why cyber security is important. Retrieved from: https://www.whitecase.com/publications/insight/cyber-risk-why-cyber-security-important (Last visited July 14, 2018)
Also, ethical concerns do continue to be an issue in the political debates.

“Kentucky Sen. Rand Paul voted nay over concerns the bill didn’t go far enough in protecting civil liberties. I have fought for several years now to end the illegal spying of the NSA on ordinary Americans,” Paul said before stalling the chamber into shutting down the program at the end of May. “The callous use of general warrants and the disregard for the Bill of Rights must end.”

Children need the special protection of their parents.

All of these remedial acts have social ethical implications here and abroad. Cyber technical actions affect self-actualization, and the cost of operating a business. The ushering in of the corporation into the new legal issues of a digital age is occurring at a rapid pace. Surprisingly, cell phone producers do have the capacity to record your conversations and listen to them from the cloud. Amazon does have the purchasing data from users. Recognizing and adjusting to the digital age technology changes has been a problem for the legal system and corporations around the world. Formal compliance ethical committees must utilized to hear evidence and provide insights to enact corporate policies insuring the exercise of reasonable care. It is up to us on an ethical basis to do the right thing, ethically.

CONCLUSIONS

1. Corporations need to be more internally responsible. We need to increase self-awareness and instead of defending various positions, act in good faith solving problems together viewing perspectives from both sides.
2. Follow the law and set appropriate parameters. Engage in reasoned decision making. Be strict when the facts apply to children.
3. Continue to unleash responsible commercial opportunities. For example, move forward in the area of artificial intelligence in a responsible way. Don’t just dump the technology on the market to make a quick dollar. Think through the ethical perspectives and allow responsible usage in all decisions. It is the best long run perspective for the investor and the stakeholders.
4. Establish ethics review boards and education programs especially for international corporations.
5. Engage customers in consent agreements. It may be a way around the civil litigation process. Signing a simple contract does inform the consumer. It has to be a simple contract for the good of society.

AUTHOR BIOGRAPHIES

Paul J. Morrow, Sr, Esq., is an associate professor of Law and Economics at Husson University with 30 years of private practice and teaching experience. He was an investment trust advisor, then a litigation attorney for a total of 17 years of private practice. In that time, he was an Assistant Attorney General. During his private practice, he taught a good number of courses then transitioned to teaching full time in 2002. He is published in Cyberlaw, Environmental law and Business Law education. His B.A. is from the University of Maine, and he earned his Juris Doctorate degree from the University of New Hampshire School of Law in 1985 where he served on the Dean’s Council in 2012 and 2013. He is a member of the Maine Bar Association serving as a member of the Corporate Law section and the Consumer and Financial Institution section. He is also a member of the Federal Bar Association. *(contact author)

Stephanie Shayne, MBA earned her undergraduate degree in Economics, with a minor in Mathematics from Colby College. She earned her Master’s degree in Business Administration from Duke University. She is currently working on her doctorate in higher education administration at Northeastern University. She has worked as a consultant in several areas including transfer pricing, healthcare and financial services. She began her teaching career at community colleges in both North Carolina and Virginia. She started working at Husson in 2009 as an adjunct instructor before joining the faculty full time in 2011. She has extensive experience in distance education, having taught online for over 15 years.

Giuseppe Macri, (2015, September). The cybersecurity and surveillance questions nobody is asking 2016 GOPers, Part 1. Retrieved from http://www.insidesources.com/the-cybersecurity-and-surveillance-questions-nobody-is-asking-2016-gopers-part-1/ (Last visited July 14, 2018)
REFERENCES

Angwin, J. (2018) Four ways to fix facebook. Retrieved from: http://business-ethics.com/2018/04/08/four-ways-to-fix-facebook/ (Last visited: July 19, 2018)

Bloomberg (2018, March) Facebook may have breached a 2011 consent agreement, FTC says. Retrieved from: http://fortune.com/2018/03/29/cambridge-analytica-facebook-scandal/ (Last visited July 9, 2018)

Brad S. Karp, Paul, Weiss, Rifkind, Wharton & Garrison LLP, (2016). Comments Off on Federal Guidance on the Cybersecurity Information Sharing Act of 2015 Retrieved from: https://corpgov.law.harvard.edu/2016/03/03/federal-guidance-on-the-cybersecurity-information-sharing-act-of-2015/ (Last visited July 9, 2018)

Brinegar v. United States, 338 U.S. 160 (1949)

Carpenter v. U.S. 2018 WL 3073916 (2018)

Carroll v. United States, 267 U. S. 132, 162 (1925)

Davis, Kristina (2015, Dec). Why cybercrime is so hard to investigate. Retrieved from: http://www.crime-research.org/articles/4002 (Last visited July 9, 2018)

D’Onfro, J. (2018, July). Facebook confirms that SEC, FBI, and FTC have asked questions about Cambridge Analytica. Retrieved from: https://www.cnbc.com/jillian-donfro/ (Last visited July 9, 2018)

Frenkel, S. & Singer, N. (2018, March). Facebook introduces central page for privacy and security settings. Retrieved from https://www.nytimes.com/2018/03/28/technology/facebook-privacy-security-settings.html (Last visited July 9, 2018)

Gabel, D., Bertrand, L., & Orzechowski, D. (2015, July). Cyber risk: Why cyber security is important. Retrieved from: https://www.whitecase.com/publications/insight/cyber-risk-why-cyber-security-important (Last visited July 14, 2018)

Giuseppe Macri, (2015, September). The cybersecurity and surveillance questions nobody is asking 2016 GOPers, Part 1. Retrieved from http://www.insidesources.com/the-cybersecurity-and-surveillance-questions-nobody-is-asking-2016-gopers-part-1/ (Last visited July 14, 2018)

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

Kentucky v. King, 563 U.S. 452, 460, 131 S.Ct. 1849, 179 L.Ed.2d 865 (2011)

Mincey v. Arizona, 437 U.S. 385, 394, 98 S.Ct. 2408, 57 L.Ed.2d 290 (1978)

Morrow, P. (2016). Assessing multinational global cyber business risk of cyberattacks –Minimizing the risk of loss due to wrongful jurisdiction. Retrieved from: https://www.cluteinstitute.com/ojs/index.php/JCR/article/view/9961/10062 (Last visited July 18, 2018)

Shear, B. (2017, December). Avoid Facebook’s new messenger app for kids to protect your family’s privacy and future. Retrieved from: https://www.studentprivacymatters.org/avoid-facebook-s-new-messenger-app-for-kids-to-protect-your-families-privacy-future/ (Last visited, July 9, 2018)

Taylor, A. (2018). Cambridge Analytica’s reach went far beyond the U.S. elections. Retrieved from: https://www.washingtonpost.com/news/worldviews/wp/2018/03/20/cambridge-analyticas-reach-went-far-beyond-the-u-s-elections/?noredirect=on&utm_term=.a649e735a58c (Last visited, July 9, 2018)

Terry v. Ohio 392 U.S. 1 (1968)