Assessing Multinational Global Cyber Business Risk Of Cyberattacks – Minimizing The Risk Of Loss Due To Wrongful Jurisdiction

Paul J. Morrow Sr, Esq. Husson University, USA

ABSTRACT

In Cyberspace, more and more, corporations with global holdings are seeking excellence in business around the world mostly by Internet. In order to do business, several legal and economic developments must be explored to assess the risks and practicalities involving the new legal issues created by cyberspace. Compliance officers, because of their responsibilities to develop cybersecurity plans, need to understand the personal jurisdictional effects test and the subject matter test to assess risk of loss. Jurisdiction as to what court or what administrative agency has authority to decide a particular case is critical to the success of a recovering party filing a lawsuit seeking damages for a cyberattack. The jurisdictional nuances analyzed in this paper offer a gradual development of the leading court and administrative cases for guidance on the issues.

This paper is worth your time because: 1) it examines the inconsistent and obscure legal standards for jurisdiction in cyber space including cyberattacks, 2) it shows the places and methods used by both the Federal Trade Commission and the Courts having jurisdiction over cyberattack litigation, 3) it gives the recommendations for U.S. and international corporations on the subject of cyber jurisdiction. All of this is supported by current case law and journal articles involving cybersecurity to help minimize the mistakes that I have observed in the practice saving time and money. This is a new technology area of inquiry facing many corporate legal departments, and IT managers today. So, this paper involves the legal/business research necessary to give guidance regarding the jurisdictional boundaries of cyberattack litigation and ways to substantially reduce the risk of loss.

Keywords: Jurisdiction; Cyberattacks; Federal Trade Commission; Cybersecurity

INTRODUCTION

The statistics regarding cybersecurity risk are staggering. Very recently. 500 million accounts were hacked at Yahoo. 45 billion dollars per year are tied to identity theft alone. Our political leaders are calling for strikes against terrorist groups. Major corporations including our government networks are under attack by hackers who want to do harm. In the wake of all of the chaos of a cyberattacks, our major institutions are not fully appraised of the standards of compliance and therefore the solutions. Cyberattacks have become prevalent. "The numbers from recent data breaches are staggering: credit card information from 56 million Home Depot and 70 million Target customers, 145 million login credentials from eBay, contact information for 76 million J.P. Morgan Chase customers and 80 million Anthem customers. Even small companies are not immune to these cyber- attacks. From card skimmers to point-of-sale intrusions, data theft rings have targeted relatively unprotected small businesses as a new and vast profit center."[1] "Given the significant cyber-attacks that are occurring with disturbing frequency, and the mounting evidence that companies of all shapes and sizes are increasingly under a constant threat of potentially disastrous cyber-attacks, ensuring the adequacy of a company's

[1] Moy, E. (2015). Cyber Attacks Pose Biggest Unrecognized Threat to Economy. Newsmax.com. Retrieved from http://www.newsmax.com/Finance/Ed-Moy/cyber-attack-terrorism-economy/2015/05/07/id/643241/ (Lasted visited September 3, 2016)

cybersecurity measures needs to be a critical part of a board of director's risk oversight responsibilities."[2] Therefore, IT directors and the directors of a corporation need to receive guidance on the sublime issue of jurisdiction. It is a heightened duty of care within the corporation to protect shareholder interest.

Many of the hidden incisive issues of lawsuits that corporations have to face from the consumer sector and other corporations in cyber security involves case law legal analysis including jurisdiction, compliance with the Federal Trade Commission regulations and the interpretation of the regulations in the courts. "One of the many big challenges many cybersecurity professionals face is embedding security into their projects. However little is rarely discussed of the challenges facing large scale, multi-jurisdictional programs - particularly in regulated industries or sectors."[3] What are the administrative standards? What are the court standards? The concept of being able to have minimum contacts with the United States as a whole has profound implications for the internet and international jurisdiction. "Users all over the world, without establishing contacts in a particular state, could establish contacts with the entire country with nearly every foray into cyberspace."[4] With appropriate recommendations that help to manage the risk, corporations may substantially reduce but not eliminate the exposure to liability.

PERSONAL JURISDICTION AND LEGAL TRANSACTIONAL ANALYSIS (COURT TRACK AND/OR ADMINISTRATIVE TRACK)

Cases can take two tracks sometimes taken together. Plaintiffs file lawsuits in the courts in the traditional way and/or the Federal Trade Commission undertakes to adjudicate a case in the federal administrative agency domain. I will first address the cases that take the court track, then I will show the nuances for the cases that take the administrative track.

If a case is heard in a court taking the court track, here is the situation. A jury awards 20 million dollars to a corporation for a cybersecurity breach. On appeal, the 20 million dollar verdict is overturned because the plaintiff corporation did not establish personal jurisdiction over the defendant corporation. This litigation strategy is classic and presents a substantial sublime risk to the assets of a corporation. Courts are having problems defining jurisdiction in cyberattack cases. As a result, boards of directors face the risk of being ill-advised because the law is so unclear. It is important that we begin the analysis with the legal analytics on this obscure but real topic of jurisdiction in cyberattacks to make corporate officials aware of the unseen risk presented by jurisdiction so that it may be properly addressed before law suits are filed. The potential impact of liability denoted from a verdict being overturned based on the technicality of jurisdiction is enormous and not well publicized until after a case has been decided. The jurisdictional legal tests are hidden in cases and administrative decisions. Not knowing the computer systems standards from the FTC, or receiving an overturned verdict based on an oversight involving jurisdiction can devastate the assets of a corporation and its board of directors.

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.

There are not many cases that give the gradual developments of jurisdiction in cyber-space. As a result, the law of jurisdiction in cyber-space is relatively unclear. The following case represents the newness of the issues in cyberspace. Exercising jurisdiction over internet transactions is imperative for our court system. "Regarding the question of where acts or omissions conducted in cyberspace actually occur, this Court, acknowledged that the law

[2] Aguilar, Luis A. (2014). Comm'r, U.S. Sec. & Exch. Comm'n, Cyber Risks and the Boardroom, Conference, *Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus*, Retrieved from http://www.sec.gov/News/Speech/Detail/Speech/1370542057946. (Lasted visited September 3, 2016)

[3] Loidl, Jarrod. (2015). Start With The End In Mind: Multi-jurisdictional cybersecurity. Cybersecurity & Technology Risk Professional. Retrieved from https://www.linkedin.com/pulse/start-end-mind-multi-jurisdictional-cybersecurity-jarrod-loidl (Lasted visited September 3, 2016)

[4] Betsey Rosenblatt, Principles of Jurisdiction, http://cyber.law.harvard.edu/property99/domain/Betsy.html,(Lasted visited September 3, 2016)

in the area of personal jurisdiction based upon an Internet presence is still evolving"[5] (Stanley Young v. New Haven Advocate, et. al.). There are plenty of rudimentary examples on this incisive issue.

THE LEGAL TEST FOR JURISDICTION OVER THE PERSON AND THE SUBJECT MATTER.

The law is best illustrated with quotes from the following leading cases. Pursuant to the fourteenth amendment's Due Process Clause, a nonresident defendant is amenable to suit in a particular forum when she has "minimum contacts" with the forum State such that maintenance of the suit does not offend traditional notions of fair play and substantial justice[6] (International Shoe v. Washington). The next leading case is Zippo and is confusing on the issue because it satisfies the minimum contact test with a totally different means to end methodology. In Zippo, personal jurisdiction, as a concept applies to the internet, and is communicated in a two part test and sliding scale thusly: "at one end of the spectrum are situations where a defendant clearly does business over the Internet. If the defendant enters into contracts with residents of a foreign jurisdiction that involve the knowing and reported transmission of computer files over the Internet, personal jurisdiction is proper. At the opposite end are situations where a defendant has simply posted information in an internet website which is accessible to users in foreign jurisdictions. A passive website that does little more than make information available to those who are interested in it is not grounds for the exercise of personal jurisdiction. The middle ground is occupied by interactive Web sites where a user can exchange information with the host computer. In these cases, the exercise of jurisdiction is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the website"[7] (Zippo Manufacturing Company v. Zippo Dot Com, Inc). The logic and reasoning is reasonably consistent with our minimum contacts test from our Constitutional foundation. But the test is a sliding scale which makes it confusing.

"At the opposite end are situations where a defendant has simply posted information on an Internet Web site which is accessible to users in foreign jurisdictions. A passive Web site that does little more than make information available to those who are interested in it is not grounds for the exercise personal jurisdiction. E.g. Bensusan Restaurant Corp., v. King, 937 F. Supp. 295 (S.D.N.Y., 1996). The middle ground is occupied by interactive Web sites where a user can exchange information with the host computer. In these cases, the exercise of jurisdiction is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the Web site. E.g. Maritz, Inc. v. Cybergold, Inc., 947 F. Supp. 1328 (E.D.Mo., 1996)."[8]

Some states apply the doctrine of jurisdiction in yet another fashion that does not include the Zippo test and goes beyond the reasoning in Zippo and its progeny. The U.S. Supreme Court noted in Burger King v. Rudzewicz, although a contract alone may not establish minimum contacts between a nonresident defendant and the jurisdiction, evaluation of the events and activities surrounding the contract and the contract terms may serve "to determine whether a defendant purposefully established minimum contacts with the forum."[9] Thus, yet another test now involving the purposeful intent of the parties.

If there is a contract involved, (such as just clicking I agree to an internet command) contract terms and the attendant circumstances, implications and inferences become relevant to the determination of jurisdiction. In Carefirst of Maryland, Incorporated, d/b/a Carfirst Blue Cross/Blue Shield v. Carefirst Pregnancy Centers, Incorporated, d/b/a Carefirst, a case involving a non-interactive website, the Federal District Court ruled "Because there is, in this case, no suggestion that CPC engaged in continuous and systematic activities with Maryland, our inquiry must focus on the conduct giving rise to the suit, i.e., CPC's alleged infringement of Carefirst's trademark. And accordingly, it is only if (1) CPC purposefully availed itself of the privilege of conducting activities in Maryland, (2) Carefirst's claims arose out of those activities, and (3) the exercise of personal jurisdiction would be constitutionally "reasonable", that CPC can be held subject to specific jurisdiction in Maryland. In conducting this inquiry, we

[5] Stanley Young v. New Haven Advocate, et.al., 184 F. Supp. 2nd 498, (2001), 29 Media L. Rep. 2609
[6] International Shoe v. Washington., 326 U.S. 310, 316, 66 S. Ct. 154, 90 L. Ed. 95 (1945).
[7] Zippo Manufacturing Company v. Zippo Dot Com, Inc., 952 F. Supp. 1119, 65 USLW 2551, 42 U.S. P.Q. 2nd 1062.
[8] Id .
[9] Burger King v. Rudzewicz, 471 U.S. 462, 472-473, 105 S. Ct. 2177, 85 L.Ed.2nd 528 (1985)

direct our focus to the quality and nature of CPC's Maryland contacts."[10] This illustrates a more functional test. A test derived by the nature of the contact.

In two other cases, Maine and New York, the Courts extend the analysis of jurisdiction. In Maine the case, Judge John Woodcock delivering the opinion of the Court in a case involving a Maine resident being injured in Virginia by a Georgia resident he states "The Maine Law Court has determined that before exercising its jurisdiction over an out-of-state defendant, the Court must conclude that (1) Maine has a legitimate interest in the subject matter of this action; (2) the defendant, by its conduct, should reasonably have anticipated litigation in Maine; and , (3) exercise of jurisdiction by Maine's courts would comport with traditional notions of fair play and substantial justice."[11] (Charlene and Robert Cormier v. James Todd Fisher).

This line of cases represents a protect the public standard. This means that the courts take a public policy approach in exercising jurisdiction. In K.C.P.L., INC., v. William Cary NASH_ a New York cyber-piracy case, the court states " At least one court has determined that jurisdiction exists over a defendant who is alleged to be a "cybersquatter" or "cyber pirate" , i.e. one who is engaged in the business of stealing valuable trademarks and registering them as domain names for purpose of selling the rights to the domain names to the trademark owners. The same court citing Panavision International, L.P. v. Toeppen states "the defendant activities amounted to a scheme to extort money from the plaintiff and constituted the "something more" required to support the exercise of personal jurisdiction in that case."[12]

If the quality of the contacts is substantial enough, the courts tend to exercise jurisdiction. However, it is not automatic. In two cases, the courts have refused to exercise jurisdiction.

"Two other recent decisions, in declining to exercise jurisdiction, support the notion that passive Internet sites are not sufficient to support jurisdiction. In McDonough v. Fallon McElligott, Inc., a Minnesota defendant had displayed plaintiff's photographs on the Web without plaintiff's consent, in possible violation of California copyright and unfair competition laws. The Southern District of California held that: "Because the Web enables easy world-wide access, allowing computer interaction via the Web to supply sufficient contacts to establish jurisdiction would eviscerate the personal jurisdiction requirement as it currently exists . . . . Thus, [having] a Web site used by Californians cannot establish jurisdiction by itself." Similarly, in Benusan Restaurant Corp. v. King, the Southern District of New York held that the operator of a small Missouri jazz club called "The Blue Note" did not subject it to New York's trademark laws by erecting an advertising site on the Web."[13]

Theoretically, within these principles, a person having a website and carrying on business in Maine may meet this three part test given that Maine has an interest in protecting its citizens from crime or torts, and that it was reasonably foreseeable that the defendant could be hauled into Court for any wrongdoing, as long as the opinion of the Court and rational ends-means test comports with the traditional notions of the due process clause of the U.S. Constitution. If the case involves an international corporation doing business in the U.S., the same case law principles apply. The bottom line is that if any corporation sends an electronic signal within the boundaries of the U.S. and there is an active business motive, a state may exercise personal jurisdiction depending on its interpretation of the due process clause. This leaves much uncertainty even if corporate legal departments do everything they can

[10] Carefirst of Maryland, Incorporated, d/b/a Carfirst Blue Cross/Blue Shield v. Carefirst Pregnancy Centers, Incorporated, d/b/a Carefirst, 334 F.3d 390, 56 Fed. R. Serv. 3d. 361, 67 U.S.P.Q. 2nd 1243 (2003), Citing Nichols v. G.D. Searle & Co., 783 F. Supp. 233,238 (D.Md.1992) Citing Nichols v. G.D. Searle & Co., 783 F.Supp. 233,238 (D.Md.1992) This Court goes on to state, This "effects test" of specific jurisdiction is typically construed to require that the plaintiff establish that : (1) the defendant committed and intentional tort; (2) the plaintiff felt the brunt of the harm in the forum, such that the forum can be said to be the focal point of the harm; and (3) the defendant expressly aimed his tortious conduct at the forum, such that the forum can be said to be the focal point of the tortuous activity." Citing IMO Indus., Inc. v. Kiekert AG, 155 F.3d 254, 265, 266 (3dCir. 1988). " Occupying the middle ground are semi-interactive websites, through which there have not occurred a high volume of transactions between the defendant and residents of the foreign jurisdiction, yet which do enable users to exchange information with the host computer. In these cases, the exercise of jurisdiction is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs." Carefirst of Maryland, Incorporated, d/b/a Carefirst Blue Cross/Blue Shield vs. Carefirst Pregnancy Centers, Incorporated, d/b/a Carefirst, 334 F.3d 390, 56 Fed. R. Serv. 3d. 361, 67 U.S.P.Q. 2nd 1243 (2003)

[11] Charlene and Robert Cormier v. James Todd Fisher 404 F. Supp.2nd 357 (Me. 2005).

[12] K.C.P.L., INC., v. William Cary NASH_1998 WL 823657 (S.D.N.Y.), 49 U.S.P.Q. 2nd 1584 (1998) Citing Panavision International, L.P. v. Toeppen 141 F3d. 1316 (9th Cir. 1998).

[13] Betsey Rosenblatt, Principles of Jurisdiction, http://cyber.law.harvard.edu/property99/domain/Betsy.html,(Lasted visited September 3, 2016)

to ferret out this issue. Obviously, this is an incredible onus to comply with the administrative standards provided by the FTC and the recommendations of this paper.

In short summary, in the court system, the world is left with the proposition as to whether a website is passive, or active and a question of purposeful intent. Also, in the mix is whether the activity rises to a level where it violates public policy so that a court is compelled to protect its citizens. If any one of these justifications are met, then there are minimum contacts. Also, each case decided depends on the precedent of cases decided at the state level within the federal common law. Corporations, domestic and international, need more clarity to plan, organize, control and assess risk. A federal administrative agency could render much help on the subject.

INTERNATIONALLY

The effects test also applies to international corporations who have a business presence in the States. Many corporations who conduct business abroad are subject to the international laws and treaties of the country in which the business in conducted. Laws vary country to country. But, many foreign corporations doing business in the U.S. face the same liability issues for internet attacks as domestic corporations. The Federal Trade Commission, on behalf of the U.S. can initiate an action on behalf of the citizens of the U.S. based upon the Wyndham Worldwide Corp case analyzed further in this paper.

THE ADMINISTRATIVE TRACK

As stated, in a recent development, there is the administrative track. Most cases start at the administrative agency level of adjudication. Subject matter jurisdiction or in other words authority to decide cyberattack cases is with the Federal Trade Commission at the administrative agency level. Personal jurisdiction is usually not much of an issue because this is a Federal Agency that has the authority to decide cases in the U.S. These cases do involve a plaintiff usually the government. When the agency itself brings the action, it is 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 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 findings, and provides a quicker more inexpensive snap-shot of the factual legal merits of a case. As stated, the issue that is usually heavily contested is whether the administrative agency had subject matter jurisdiction, or authority to decide the case in the first place. If not, then the case gets dismissed usually with no repercussions. If this happens, 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 to the case filed in court.

The subject matter jurisdictional analysis for the Federal Trade commission starts with the following leading cases. First there is the case of Cardsystems Solutions, Inc. "According to the FTC, CardSystems provided merchants with products and services used in "authorization processing" – obtaining approval for credit and debit card purchases from the banks that issued the cards. Last year, it processed about 210 million card purchases, totaling more than $15 billion, for more than 119,000 small and mid-size merchants. In processing these transactions, CardSystems collected personal information from the magnetic strip of the card, including the card number, expiration date, and other data. CardSystems then stored this information on its computer network. Pay By Touch acquired CardSystems' assets in December 2005, and now processes transactions for the same merchants CardSystems served."[14] The FTC brought the action.

[14]Federal Trade Commission Press Release https://www.ftc.gov/news-events/press-releases/2006/02/cardsystems-solutions-settles-ftc-charges, (last visited September 7, 2016)

Quickly getting to the ruling of the FTC, the agency ruled "The acts and practices of the respondent as alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act."[15]

Therefore, the FTC has authority to decide and rule on cyberattack cases and did exercise jurisdiction over the Cardsystems cyber-matter. The personal jurisdiction issue was not raised by the defendant at the FTC level because as previously stated, at the FTC level, personal jurisdiction is usually not a big issue. Following the authoritative logic that the courts do have the final say, the Cardsystems case was affirmed by the courts in the case of Federal Trade Commission v. Wyndham Worldwide Corp. The FTC issued the complaint and the decision, stating that the FTC has subject matter jurisdiction over cyberattacks and the FTC has promulgated the standards to follow by IT departments which was affirmed in the case Federal Trade Commission v. Wyndham Worldwide Corp.

The federal circuit court in the Wyndham case considered the subject matter jurisdictional aspects of the case which were resolved favorably for the court to hear the appeal from a case heard first at the Federal Trade Commission because the commission ruled in Cardsystems Solutions, Inc. the FTC had the jurisdiction to promulgate the standards that corporations and their directors need to follow. In the court case Wyndham, testing the administrative case, Cardsystems, the salient facts are briefly stated as follows:

"On three occasions in 2008 and 2009 hackers successfully accessed Wyndham Worldwide Corporation's computer systems. In total, they stole personal and financial information for hundreds of thousands of consumers leading to over $10.6 million dollars in fraudulent charges. The FTC filed suit in federal District Court, alleging that Wyndham's conduct was an unfair practice and that its privacy policy was deceptive. The District Court denied Wyndham's motion to dismiss, and we (FTC) granted interlocutory appeal on two issues: whether the FTC has authority to regulate cybersecurity under the unfairness prong of § 45(a); and, if so, whether Wyndham had fair notice its specific cybersecurity practices could fall short of that provision. We affirm the District Court."[16] Federal Trade Commission v. Wyndham Worldwide Corp.

The literal findings of the court are as follows: "The Federal Trade Commission Act prohibits "unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. § 45(a). In 2005, the Federal Trade Commission began bringing administrative actions under this provision against companies with allegedly deficient cybersecurity that failed to protect consumer data against hackers. The vast majority of these cases have ended in settlement."[17]

The Federal Trade Commission has regulatory jurisdiction over the practical procedures for corporations to follow. The court in the aforementioned case lays out the corporate protocol by ruling on the issue of notice: "Having decided that Wyndham is entitled to notice of the meaning of the statute, we next consider whether the case should be dismissed based on fair notice principles. We do not read Wyndham's briefs as arguing the company lacked fair notice that cybersecurity practices can, as a general matter, form the basis of an unfair practice under § 45(a). Wyndham argues instead it lacked notice of what *specific* cybersecurity practices are necessary to avoid liability. We have little trouble rejecting this claim."[18] So, the court rejected Wyndham's arguments.

The federal court found that the FTC did have jurisdiction over the matter. Therefore, the court had authority to decide the case.

Ultimately, in Wyndham, Judge Ambro basically ruled that:

1. The company's alleged failure to maintain reasonable and appropriate data security, if proven, could constitute an unfair method of competition in commerce;
2. subsequent Congressional acts did not cause Federal Trade Commission Act (The Act) provision prohibiting unfair practices to exclude **cybersecurity** issues; and
3. the company had fair notice of the meaning of provision of Act prohibiting unfair practices.

[15] In the Matter of Cardsystems Solutions., a corporation, credit card case. 2006 WL 2709787Docket No. C-4168 (September 5, 2006).
[16] Federal Trade Commission v. Wyndham Worldwide Corp, 799 Fed App .3rd 236 3rd Circuit, (2015).
[17] Id.
[18] Id.

CONCLUSIONS

All in all, it is difficult to fathom that our framers ever could have imagined how developed a society we would become and that the true fundamental tenets of the cases that were decided one after another by the arduous work of many dedicated attorneys, and internal strife that even today challenging questions on the frontier of internet law still require us to analyze cases carefully for the sake of ordered liberty. Although this area of the law is complex and challenging, we must think and comport with our Constitutional elders and the system is desperately trying to achieve a good result.

How the courts define minimum contacts will affect how society is held responsible for internet transactions. It remains to be determined if clicking "I agree" to an internet contract renders jurisdiction. Whether we should use an ends-means type of test or an active/passive website test or a sliding scale (Zippo) still leaves many questions unanswered. As a matter of public policy, the States have a compelling interest in protecting its citizens from out of state internet users. This interest does rise to a level where the three part test currently used in the Maine Courts clearly leads the way in protecting not only the legitimate interest of the parties, but the interest of the residents and citizens of the affected State. If the minimum contacts test is met, a court may only exercise jurisdiction if it is "reasonable" to do so. In determining reasonableness, a court must weigh and consider the burden on the defendant to litigate in the forum, the forum state's interests in the matter, the interest of the plaintiff in obtaining relief, efficiency in resolving the conflict in the forum, and the interests of several states in furthering certain fundamental social policies. In essence, jurisdiction for cyberattacks is really up to a particular court. Also, on the administrative track, the FTC test is more definitive. Following the decisions from the FTC may be a more relevant guide and provide more clarity.

"In sum, under U.S. law. if it is reasonable to do so, a court in one state will exercise jurisdiction over a party in another state or country whose conduct has substantial effects in the state and whose conduct constitutes sufficient contacts with the state to satisfy due process. Because this jurisdictional test is ambiguous, courts in every state of the U.S. may be able to exercise jurisdiction over parties anywhere in the world, based solely on Internet contacts with the state."[19]

Private parties are encouraged where possible through forum selection clauses and arbitrations clauses to secure a jurisdictional position. The laws of each state vary immensely with respect to liability. In future cases, we can be certain that in some cases the courts will nullify the jurisdictional decision of the FTC. As a result, the question of who has jurisdiction still remains a mystery and is still shrouded in the conflict of laws and cases yet to be presented.

Strategic recommendations to reduce risk of loss:

1. Upgrade computer systems immediately (with specialty consultants) to meet the FTC standards and buy cyberattack insurance.
2. Arbitrate and mediate all disputes to avoid litigation. Include the arbitration/mediation clauses is all contracts for protection.
3. Include forum selection clauses in all contracts.
4. Accept the fact that the FTC has jurisdiction, know the standard and comply. If questioned, you will have something to show the FTC your reasonable efforts to comply.
5. Negotiate jurisdiction, especially for international firms, by signing contracts that specify which state will have authority to decide cases. Pick a state that has favorable laws.
6. Be very active in technology on the recent development of cases that affect jurisdiction. It is a fiduciary duty and an affirmative defense in negligence cases against the directors of the corporation.

[19] Betsey Rosenblatt, Principles of Jurisdiction, http://cyber.law.harvard.edu/property99/domain/Betsy.html (Lasted visited September 3, 2016)

AUTHOR BIOGRAPHY

Paul J. Morrow, Sr, Esq., is an associate professor of Law and Economics at Husson University with 30 years of combined private practice and teaching experience. He was an investment trust advisor, then a litigation attorney for a total of 17 years of private practice. During the time of his private practice, he taught a good number of courses transitioning to teaching full time in 2002. He is published in Cyber-law, 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. 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. E-mail: morrowp@husson.edu

REFERENCES

Aguilar, Luis A. (2014). Comm'r, U.S. Sec. & Exch. Comm'n, Cyber Risks and the Boardroom, Conference, *Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus*, Retrieved from http://www.sec.gov/News/Speech/Detail/Speech/1370542057946.

Betsey Rosenblatt, Principles of Jurisdiction, http://cyber.law.harvard.edu/property99/domain/Betsy.html

Burger King v. Rudzewicz, 471 U.S. 462, 472-473, 105 S.Ct. 2177, 85 L.Ed.2nd 528 (1985)

Carefirst of Maryland, Incorporated, d/b/a Carfirst Blue Cross/Blue Shield vs. Carefirst Pregnancy Centers, Incorporated, d/b/a Carefirst, 334 F.3d 390, 56 Fed. R. Serv. 3d. 361, 67 U.S.P.Q. 2nd 1243 (2003)

Charlene and Robert Cormier v. James Todd Fisher 404 F. Supp.2nd 357 (Me. 2005).

Federal Trade Commission Press Release https://www.ftc.gov/news-events/press-releases/2006/02/cardsystems-solutions-settles-ftc-charges,(last visited September 7, 2016)

Federal Trade Commission v. Wyndham Worldwide Corp, 799 Fed App .3rd 236 3rd Circuit, (2015).

In the Matter of Cardsystems Solutions., a corporation, credit card case. 2006 WL 2709787Docket No. C-4168 (September 5, 2006).

International Shoe v. Washington., 326 U.S. 310, 316, 66 S.Ct. 154, 90 L.Ed. 95 (1945).

K.C.P.L., INC., v. William Cary NASH_1998 WL 823657 (S.D.N.Y.), 49 U.S.P.Q. 2nd 1584 (1998) Citing Panavision International, L.P. v. Toeppen 141 F3d. 1316 (9th Cir. 1998).

Loidl, Jarrod. (2015). Start With The End In Mind: Multi-jurisdictional cybersecurity. Cybersecurity & Technology Risk Professional. Retrieved from https://www.linkedin.com/pulse/start-end-mind-multi-jurisdictional-cybersecurity-jarrod-loidl.

Moy, E. (2015). Cyber Attacks Pose Biggest Unrecognized Threat to Economy. Newsmax.com. Retrieved from http://www.newsmax.com/Finance/Ed-Moy/cyber-attack-terrorism-economy/2015/05/07/id/643241/

Stanley Young v. New Haven Advocate,et.al. , 184 F.Supp. 2nd 498, (2001), 29 Media L. Rep. 2609

Zippo Manufacturing Company v. Zippo Dot Com, Inc., 952 F. Supp. 1119, 65 USLW 2551, 42 U.S. P.Q. 2nd 1062.