FTC REGULATING CYBERSECURITY POST *WYNDHAM*: AN INTERNATIONAL COMMON LAW COMPARISON ON THE IMPACT OF REGULATION OF CYBERSECURITY

Andrew Zachery Ryan Smith[*]

TABLE OF CONTENTS

---

[*] J.D., University of Georgia, 2017; B.A, Michigan State University, *with honors*, 2012. I would like to thank Professor Barnett for his considerable guidance in writing this Note.

I. INTRODUCTION

What happens to all that information you are required to provide to Amazon when you buy that new shirt? Do they keep your address, credit card number, and phone number on a secure, encrypted server? When you accept the user-agreement for iTunes, which you undoubtedly fail to read, what protections does Apple provide to keep your information safe? As consumers increasingly use the internet to make everyday purchases and businesses increasingly collect and store consumer information, protections need to be put in place to ensure that this information is stored in a way that limits and prevents threats from cybercrime.

An October 2015 study by the Ponemon Institute determined that the average annual cost of cybercrime in the United States is $15.42 million per United States company—an increase from $12.69 million only a year ago.[1] As the threat of cybersecurity breaches to consumers continues to increase, and costs associated with that threat continue to rise, businesses must find ways to mitigate these damages. But when businesses fail to provide adequate protections, should the government step in? In response to the myriad of attacks, the Federal Trade Commission (FTC) may be the regulatory arm of the federal government with the arsenal to affect the change needed to combat the millions of dollars spent every year on cybercrime. But does the FTC have the authority to hold businesses accountable? A mixture of administrative adjudications and a recent court decision suggest that it does.

Recently, the Third Circuit ruled that the FTC has the authority under the unfairness prong of the Federal Trade Commission Act[2] (FTCA) to regulate and fine businesses that lose consumer information to hackers where the company fails to provide adequate safeguards to the businesses' consumer information stored online.[3] The decision stems from the FTC's decision to sue Wyndham Hotels for allowing three cyberattacks that resulted in the theft of more than 600,000 consumers' credit card information and over $10 million in fraudulent charges.[4] This is not the first time that the FTC has gone after businesses for issues related to cybersecurity; in fact, the FTC has settled over fifty cases against companies for cybersecurity matters,

---

[1] Ponemon Institute, *2015 Cost of Cyber Crime Study* (Oct. 2015), https://ssl.www8.hp.com/ww/en/secure/pdf/4aa5-5207enw.pdf.

[2] *See* 15 U.S.C. § 45(a)(1) (2006) (prohibition against "unfair methods of competition in or affecting commerce").

[3] FTC v. Wyndham Worldwide Corp, 799 F.3d 236 (3d Cir. 2015).

[4] *Id.* at 240.

including SnapChat Inc., Reed Elsevier Inc., and Credit Karma Inc.[5] Wyndham is the first to challenge the FTC's blanket authority, refusing to succumb to pressures to settle.

Companies found liable under the unfairness prong of the FTCA could face the multitude of tools available to the FTC, and, given that the threats of cybersecurity show no signs of slowing down, businesses simply cannot ignore the potential liability. In short, this decision may have serious consequences for companies like Wyndham that store consumer information—far greater than upset consumers and public embarrassment.[6] On September 15, 2015, Experian disclosed that an unauthorized party had hacked its system, subjecting data collected between September 2013 and September 2015 to potential fraudulent exposure.[7] While this hack did not obtain credit card information, it did collect a variety of highly sensitive information, including names, addresses, Social Security numbers, dates-of-birth, and identification numbers found on drivers' licenses, military IDs, and passports.[8] This breach prompted three U.S. Senators to demand answers from Experian and may eventually lead to liability, much like the potential liability faced by Wyndham.[9]

> U.S. Sen. Sherrod Brown (D-OH) — ranking member of the U.S. Senate Committee on Banking, Housing, and Urban Affairs — today demanded answers from Experian, the world's largest credit monitoring firm, on actions the company is taking to address the recent security breach that exposed sensitive personal data of about 15 million T-Mobile customers.[10]

And the list goes on: Primera Blue Cross, in March of 2015, was breached, exposing 11 million customers' names, dates-of-birth, Social Security numbers, mail and e-mail addresses, phone numbers, and bank

---

[5] *See* Sophia Pearson, *Wyndham Must Face Hacker Suit as Court Upholds FTC Power*, BLOOMBERG TECH. (Aug. 24, 2015), http://www.bloomberg.com/news/articles/2015-08-24/wyndham-must-face-ftc-suit-for-failing-to-stop-russian-hackers.

[6] *See generally* Andy Greenberg, *Court Says that FTC can Slap Companies for Getting Hacked*, WIRED (Aug. 24, 2015), http://www.wired.com/2015/08/court-says-ftc-can-slap-companies-getting-hacked/.

[7] Eric Chabrow, *Experian Hack Slams T-Mobile Customers*, DATA BREACH TODAY (Oct. 1, 2015), http://www.databreachtoday.com/experian-hack-slams-t-mobile-customers-a-8563.

[8] *Id.*

[9] Press Release, U.S. Sen. Sherrod Brown (OH), Brown Presses Experian for Answer Following Security Breach of 15 Million Consumers' Personal Data (Oct. 14, 2015), http://www.brown.senate.gov/newsroom/press/release/brown-presses-experian-for-answer-following-security-breach-of-15-million-consumers-personal-data.

[10] *Id.*

account information and Anthem, in February 2015, permitted 80 million records of current and former customers (and employees) to be breached, allowing access to names, Social Security numbers, dates-of-birth, addresses, e-mail, and employment information (including income data).[11]

While the cost of having greater security measures will undoubtedly increase the internal costs to businesses and eventually be passed on to the consumer, a response from the FTC to these ever-increasing cyber-related crimes seems to be imminent, given the circumstances. And while consumers may bear the eventual cost of better cyber protection, it is conceivable that increased protections may diminish or severely undercut the costs already borne by consumers as the result of the ongoing cyberattacks.

This Note aims to provide a deeper understanding of the current status of cybercrime in the United States, the United Kingdom, and Australia. By analyzing these common law countries' regulatory and statutory schemes aimed at combatting cybercrime, this Note attempts to explore whether the United States can, and should, allow the FTC to regulate businesses' cybersecurity protections. Part II of this Note discusses the recent Third Circuit opinion, which arguably strengthens the FTC's position that it has the right to assess and fine businesses that fail to provide adequate safeguards promised to consumers. Part III provides a synopsis of opinions after the Third Circuit decision to highlight the relevant concerns regarding business and consumer information as it relates to the collection of consumer protection.

Part IV provides a basis for comparison, by examining what other common law countries, particularly Australia and the United Kingdom, are doing to combat cybercrime. This includes exploring the statutory and regulatory schemes of both countries to see whether the concerns regarding FTC regulatory oversight have merit, and whether governmental regulation seems to provide the necessary supervision to combat cybercrime. Moreover, this section explores some cases in each country to determine how the respective courts are involved in this process.

Part V makes suggestions about what the government should be doing to effectively hold businesses accountable, while also encouraging businesses to adopt systems that can undercut attackers' ability to take sensitive information stored online. Finally, Part VI provides a brief conclusion with some final thoughts about how *Wyndham* may help bring about the necessary change for the United States to effectively target computer hackers.

---

[11] *See* Kevin Granville, *9 Recent Cyberattacks Against Big Businesses*, N.Y. TIMES (Feb. 5, 2015), http://www.nytimes.com/interactive/2015/02/05/technology/recent-cyberattacks.html?_r=0.

II. BACKGROUND AND PROCEDURAL HISTORY OF *FTC V. WYNDHAM*

In order to provide a deeper understanding of the FTC's ability to regulate cybersecurity—particularly as compared to what other common law countries like Australia and the United Kingdom are doing to regulate these threats—it is important to understand how the FTC is holding businesses accountable. Until 2014, no company had seriously resisted the FTC's decision to hold businesses responsible under the unfairness prong of the FTCA.[12] This section provides the backdrop for comparing how the respective regulatory and judicial entities of each country fare when dealing with cybersecurity breaches as the result of inadequate safeguards by businesses.

As such, this section explores the Third Circuit opinion *FTC v. Wyndham Hotels*, starting first with the factual background, then examining how the Third Circuit dealt with the three arguments made by Wyndham. The Third Circuit agreed to hear an immediate 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 that its specific cybersecurity could fall short of that provision."[13]

A. Wyndham's Cybersecurity Breaches

Wyndham Worldwide, a hospitality company that manages hotels and sells timeshares through subsidiaries, licensed its brand name to approximately ninety independently owned hotels.[14] Each of these hotels utilized a property management system that stored a variety of consumer information, including names, home addresses, e-mail addresses, telephone numbers, credit card numbers, expiration dates, and security codes.[15] This information was stored in a system that according to the FTC, would easily allow it.[16] Notably, the system stored this information in an unencrypted clear readable text format without any sort of firewall in place to limit

---

[12] *See* Alison Grande, *LabMD Ruling Puts FTC in Driver's Seat on Data Security*, LAW360 (May 13, 2014, 8:41 PM), https://www.bakerdonelson.com/files/Uploads/Documents/Law360%20-%20Brad%20Clanton%20quote%205-13-14%20LabMD%20Ruling%20Puts%20FTC%20In%20Driver's%20Seat%20On%20Data%20Security.pdf.

[13] FTC v. Wyndham Worldwide Corp, 799 F.3d 236, 240 (3d Cir. 2015).

[14] *Id.*

[15] *Id.*

[16] *Id.* at 240–41 (according to the FTC complaint, this included: (1) storing information in clear, readable text; (2) easy-to-guess passwords to storage systems; (3) lack of firewalls; (4) easily accessible information through non-secure servers; (5) and poor incident response procedures, among others).

access.[17] As the FTC charged, the system, developed by Micros Systems, Inc., allowed someone to easily predict the log-in credentials since the user ID and password were both "micros."[18]

On three separate occasions throughout 2008 and 2009, hackers accessed Wyndham's system with relative ease. First, in April 2008, hackers broke into the local network of an Arizona hotel that was connected to Wyndham's internet network.[19] This enabled the hackers to obtain the information of over 500,000 consumers' accounts, which they then sent to a domain in Russia.[20] Then, in March 2009, hackers gained access through an administrative account and obtained unencrypted credit card information for nearly 50,000 consumers from nearly forty hotels.[21] It was not until this point that Wyndham discovered "memory-scraping malware" that was used in the previous attack on more than thirty hotel computer systems.[22] The hackers made the third attack in March 2009, again through the use of an administrator account on one of the company's networks.[23] Wyndham only learned of this final attack in January 2010, after receiving a number of complaints from cardholders about fraudulent activity.[24] In this third attack, the hackers obtained credit card information for over 69,000 consumers from almost thirty hotels.[25] According to the FTC, during the course of the three attacks, the hackers obtained credit card information from over 619,000 consumers, resulting in at least $10.6 million in fraudulent transactions.[26] Given these inadequate safeguards, the FTC maintained that Wyndham failed to employ "reasonable measures to detect and prevent unauthorized access" to its computer network or to "conduct security investigations."[27]

Wyndham's published privacy policy, however, touts that the company promises to use encryption, firewalls, and other safeguards to protect consumer data; likewise, it states that the company safeguards consumer data "using industry-standard practices."[28] The FTC argues that this lack of security despite affirmations to the contrary amounts to an "unfair" business

---

[17] *Id.* at 241.
[18] *Id.* (paragraph 24 of the FTC complaint).
[19] *Id.* at 240.
[20] *Id.* at 241–42.
[21] *Id.* at 242.
[22] *Id.*
[23] *Id.*
[24] *Id.*
[25] *Id.*
[26] *Id.*
[27] *Id.* at 258.
[28] *Id.* at 241 (paragraph 21 of the FTC complaint); for the full language of the privacy policy, see Wyndham Hotel Group, LLC, *Privacy Policy*, https://m.wyndham.com/about/privacy-policy.html (last visited Dec. 19, 2016).

practice in violation of the FTCA's unfairness prong.[29] While Congress currently has a number of bills in consideration that would establish national standards for protecting consumer data, until any legislation is in place these FTC decisions will be establishing national security standards.[30]

B. Third Circuit Decision

On August 24, 2015, the Third Circuit in *FTC v. Wyndham Worldwide Corp*[31] determined that the FTC has broad power to regulate cybersecurity under the FTCA unfairness prong.[32] In order for the FTC to advance under this prong, it must show three factors: (1) that the injury was substantial; (2) that the countervailing benefits to consumer or competition are not outweighed; and (3) that the injury was one that a reasonable consumers could not have avoided.[33] In 1994, Congress codified this test directly into the FTCA:

> The Commission shall have no authority under this section . . . to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition. In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination.[34]

---

[29] *Id.* at 240 (quoting 15 U.S.C. § 45(a)(1) (2006)).

[30] Some of the proposed legislation includes the Cyber Intelligence Sharing and Protection Act (originally introduced as H.R. 3523—it was reintroduced in 2015 as H.R. 234 and has been referred to two committees for consideration), which was introduced in the House, and the Cybersecurity Information Sharing Act (originally introduced as S. 2588—reintroduced as S. 754 in March 2015 and is under consideration by the Senate Select Committee on Intelligence), introduced in the Senate.

[31] 799 F.3d at 236.

[32] *See* 15 U.S.C. § 45(a)(1) (2006).

[33] Originally this provision was part of a policy statement issued in 1980 that was appended to *International Harvester Co.*, 104 F.T.C. 949, 1070 (1984). The current language was codified at 15 U.S.C. § 45(n) in 1994 as part of the FTCA Amendments of 1994, Pub. L. No. 103-312, § 9, 108 Stat. 1691, 1695.

[34] 15 U.S.C. § 45(n); Pub. L. No. 103-312, § 9, 108 Stat. 1691, 1695 (1994 Amendment).

According to Wyndham, the FTC does not have authority to regulate a business's cybersecurity for three main reasons: (1) the plain meaning of unfairness does not apply to cybersecurity; (2) congressional intent and action have diminished the FTC's ability to regulate cybersecurity under the FTCA; and (3) the FTCA has failed to provide fair notice to businesses as to what constitutes adequate protection.[35]

1. Plain Meaning of Unfairness

First, Wyndham argued that the "three requirements of 15 U.S.C. § 45(n) are necessary but insufficient conditions of an unfair practice and the plain meaning of the word 'unfair' imposes independent requirements that are not met here."[36] The court acknowledged that "arguably" § 45(n) may not identify all the requirements for an unfairness claim and that "this analysis of unfairness encompasses some facts relevant to the FTC's deceptive practices claim."[37] Nonetheless, the court opined that since unfairness and deception claims frequently overlap, the court "cannot completely disentangle the two theories";[38] therefore, so long as Wyndham's conduct satisfies the reasonably avoidable requirements by way of the privacy policy, then an inference can be made that the policy was unfair to consumers.[39]

Next, Wyndham posited "that a business does not treat its customers in an unfair manner when the business itself is victimized by criminals."[40] The court quickly dismissed this argument by noting first that there is no authority to support this proposition; but then, relying on the express language of the Act, the court noted that the FTCA expressly contemplates the possibility that a business's conduct could be considered unfair before any actual injury results.[41]

Finally, Wyndham maintained that if the FTC's unfairness authority extends to Wyndham's conduct, then the FTC will effectively have the ability to "regulate the locks on hotel room doors" or even "sue supermarkets

---

[35] *Wyndham*, 799 F.3d at 244 (plain meaning); *id.* at 247 (subsequent congressional action); *id.* at 249 (fair notice).

[36] *Id.* at 244.

[37] *Id.* at 244–45.

[38] *Id.* at 245, *citing Am. Fin. Servs. Ass'n v. FTC*, 767 F.3d 957, 980 n.27 (D.C. Cir. 1985) ("The FTC has determined that . . . making unsubstantiated advertising claims may be both an unfair and a deceptive practice."), and *Orkin Exterminating Co. v. FTC*, 849 F.3d 1354, 1366 (11th Cir. 1988) ("[A] practice may be both deceptive and unfair . . . .").

[39] *Wyndham*, 799 F.3d at 246.

[40] *Id.* (internal quotations omitted).

[41] *Id.* (citing 15 U.S.C. § 45(n): "[An unfair act or practice] causes or is *likely to cause* substantial injury.").

that are sloppy about sweeping up banana peels."[42] The court sharply rejected this argument, noting that "it invites the tart retort that, were Wyndham a supermarket, leaving so many banana peels all over the place that 619,000 customers fall hardly suggests it should be immune from liability under § 45(a)."[43] Accordingly, the court determined that it was "not persuaded by Wyndham's arguments that the alleged conduct falls outside the plain meaning of 'unfair.' "[44]

2. Congressional Intent and Action

Wyndham next argued that the Fair Credit Report Act,[45] the Gramm-Leach-Bliley Act,[46] and the Children's Online Privacy Protection Act[47] have "reshaped [the unfairness prong's] meaning to exclude cybersecurity"—in short, "Wyndham concludes that Congress excluded cybersecurity from the FTC's unfairness authority by enacting these [three] measures."[48] After briefly discussing each of the three Acts, the Third Circuit determined that none of the recent privacy legislation diminishes the FTC's ability to regulate just because the FTC already has some authority to regulate corporate cybersecurity.[49]

Wyndham then argued that the FTC's decision to bring this action under the unfairness prong is "inconsistent with its repeated efforts to obtain from Congress the very authority it purports to wield here."[50] After discussing various policy decisions from the late 1990s and early 2000s, where the FTC acknowledged that it could not require businesses to adopt fair information practice policies, the court found "that the FTC later brought unfairness actions against companies whose inadequate cybersecurity resulted in consumer harm is not inconsistent with the agency's earlier position."[51] Therefore, "[h]aving rejected Wyndham's arguments that its conduct cannot

---

[42] *Id.* (internal quotations omitted).
[43] *Id.* at 247.
[44] *Id.*
[45] *See* Pub. L. No. 108-159, § 216(a), 117 Stat. 1952, 1985–86 (2003); codified as amended at 15 U.S.C. § 1681w.
[46] *See* Pub. L. No. 106-102, § 501(b), 113 Stat. 1338, 1436–37 (1999); codified as amended at 15 U.S.C. § 6801(b).
[47] *See* Pub. L. No. 105-277, § 1303, 113 Stat. 2681, 2681, 2730–32 (1998); codified as amended at 15 U.S.C. § 6502).
[48] *Wyndham*, 799 F.3d at 247.
[49] *Id.* at 247–49.
[50] *Id.* at 248.
[51] *Id.* at 249.

be unfair [the court] assume[d] for the remainder of [the] opinion that it was [fair]."[52]

3. Fair Notice

Finally, Wyndham relied on an argument espoused by most companies under attack by the FTC: that the § 45(a) does not provide "fair notice" of the cybersecurity standards it was required to implement. Here, Wyndham's argument focused on the FTC's motion to dismiss order in *LabMD*,[53] an administrative case in which the agency is pursuing an unfairness claim based on allegedly inadequate cybersecurity, protections.[54] In short, Wyndham advanced a number of arguments, all of which seek to deny the FTC *Chevron* deference[55] based on the *LabMD* case. Despite the seven separate sub-arguments that Wyndham made regarding *Chevron* deference, the Third Circuit determined that since the District Court concluded the FTC had advanced a claim under § 45(a) based on an interpretation of the statute and without any reference to *LabMD* or any other adjudication, this argument was unavailing.[56] As such, the "relevant question" became "whether Wyndham had fair notice that its conduct could fall within the meaning of the statute."[57] The court determined that Wyndham's briefs argued that the company "lacked notice of what *specific* cybersecurity practices [were] necessary to avoid liability."[58] The court had "little trouble rejecting this claim." Given that the unfairness prong does not involve any constitutional rights, it is a civil rather than criminal statute, and it regulates economic activity, the court determined that "Wyndham [was] entitled to a relatively low level of statutory notice."[59] Given the arguments advanced by Wyndham, the Third Circuit determined that the fair notice had to be "reviewed as an as-applied challenge."[60] Under this challenge, the court found that the cost-benefit analysis fell in favor of the FTC.[61]

---

[52] *Id.*

[53] *In re LabMD, Inc.*, 2015 WL 5304118 (F.T.C. 2015).

[54] *Id.* at 253.

[55] A reference to an agency's authority to fill gaps in a statutory scheme; in short, allowing the agency that is primarily responsible for interpreting the statute to fill gaps because the courts must defer to any reasonable construction it adopts. *See* Chevron, U.S.A., Inc. v. Natural Res. Def. Council, Inc., 467 U.S. 837 (1984).

[56] *Wyndham*, 799 F.3d at 253–54.

[57] *Id.* at 255.

[58] *Id.*

[59] *Id.*

[60] *Id.* at 256. For a deeper understanding of "as-applied challenges," see *United States v. Mazurie*, 419 U.S. 544, 550 (1975).

[61] *Wyndham*, 799 F.3d at 256.

The Third Circuit rejected Wyndham's arguments, maintaining that:

> [A] company does not act equitably when it published a privacy policy to attract customers who are concerned about data privacy, fails to make good on that promise by investing inadequate resources in cybersecurity, exposes it unsuspecting customers to substantial financial injury, and retains the profits of their business.[62]

It is not exactly clear why the FTC did not advance this claim under its deceptive prong,[63] since, particularly in the case of Wyndham, the FTC could plausibly argue that the privacy policy posted on the website was deceptive to consumers. The Third Circuit's analysis seemingly finds that the FTC could have brought an action against Wyndham under either the deceptive or unfairness prong.[64] Moreover, as one article suggests, "[d]eception claims are standard fare in the 50 plus cybersecurity consent decrees that the FTC has obtained to date, as well as in hundreds of other FTC consumer protection actions, most notably in the advertising and marketing context."[65] Arguably, the most likely reason that the FTC has begun bringing cybersecurity related enforcement actions under the unfairness prong is because, unlike the deception prong, no faulty representation must be shown by the FTC in order to advance a claim under the unfairness prong.[66]

The dispute is far from over. The Third Circuit only addressed whether the FTC had standing to enforce this action; the court's determination simply allows the case to proceed at the district court level. To that end, Wyndham maintains that the company did right by its consumers:

> Once the discovery process resumes, we believe the facts will show the FTC's allegations are unfounded. Safeguarding personal information remains a top priority for our company,

---

[62] *Id.* at 245.

[63] 15 U.S.C. § 45(a) (2006); see also *Wyndham*, 799 F.3d at 259, n.4 for additional insight regarding the relationship between the unfair and deceptive prongs of the Federal Trade Commission Act.

[64] *Wyndham*, 799 F.3d at 245.

[65] *See* Aravind Swaminathan, Antony P. Kim & Emily S. Tabatabai, *Third Circuit to Wyndham (Part II)*, ORRICK (Sept. 10, 2015), https://www.orrick.com/Events-and-Publications/Pages/Third-Circuit-to-Wyndham-Part-II-Deceptive-is-also-Unfair-in-the-Cybersecurity-Context.aspx.

[66] *See* J. Howard Beales, Former FTC Director, The FTC's Use of Unfairness Authority, presented at the Marketing and Public Policy Conference (May 30, 2003), https://www.ftc.gov/public-statements/2003/05/ftcs-use-unfairness-authority-its-rise-fall-and-resurrection.

> and with the dramatic increase in the number and severity of cyberattacks on both public and private institutions, we believe consumers will be best served by the government and businesses working together collaboratively rather than as adversaries.[67]

Given this relatively new practice by the FTC, many have begun to question—much like Wyndham Hotels—whether the FTC has the authority to hold businesses accountable under the unfairness prong. Additionally, the FTC's added push to go after businesses who have failed to adequately safeguard consumer information may have significant consequences on businesses' financial overhead and, invariably, on the costs borne by consumers. Much debate has circulated after the Third Circuit's decision and the next section examines part of that debate.

III. POST-*WYNDHAM* CRITIQUE

The Third Circuit's decision faced mixed reviews. Some argue that the decision is far too expansive, effectively broadening the FTC's reach beyond congressional intent. Others have praised the decision, finding that the court's assessment is consistent with the purposes of the FTCA and is necessary given the nature of consumer transactions in modern society.

According to Alan Butler, an attorney for Electronic Privacy Information Center who filed an amicus brief in *Wyndham*, "[t]his is a huge victory for the FTC, but also for American consumers [since we continue to] see services and companies being hacked on an almost daily basis now. Having the FTC out there, bringing actions against companies that fail to protect consumers' data is a critical tool."[68] To others, the Third Circuit's decision merely dispels any confusion about the FTC's ability to be a "data security watchdog."[69] As Berkeley Law Professor Chris Hoofnagle put it, "[t]he law has always imposed responsibility on companies for the care of their customers. When you're in the restaurant you have to protect against slips

---

[67] Statement by Michael Valentino, Vice President of Marketing and Communications at Wyndham. *See* John K. Higgins, *Court Bolsters FTC's Authority to Regulate Cybersecurity*, E-COMMERCE TIMES (Sept. 16, 2015), http://www.ecommercetimes.com/story/82496.html.

[68] *See* Greenberg, *supra* note 6.

[69] Alison Grande, *3rd Circ. Backs FTC in Data Security Row with Wyndham*, LAW360 (Aug. 24, 2015, 12:10 PM), https://www.law360.com/articles/664545/3rd-circ-backs-ftc-in-data-security-row-with-wyndham.

and falls or food-borne illness."[70] Now, "[d]ata is just something new that companies have to protect if they want to bear the benefits of collecting it."[71]

FTC Chairperson Edith Ramirez maintains that the decision "reaffirms the FTC's authority to hold companies accountable for failing to safeguard consumer data . . . it is not only appropriate, but critical that the FTC has the ability to take action on behalf of consumers when companies fail to take reasonable steps to secure sensitive consumer information."[72] According to Eric Chiu, the President and Co-founder of HyTrust, a cloud security automation company specializing in security, compliance, and control software,[73] "[c]onsumers have been paying the price for security breaches for too long. Hopefully, the FTC can help put greater pressure on companies to do the right thing."[74]

In a statement issued after the Third Circuit's decision, Wyndham criticized the court, stating "we continue to contend that the FTC lacks the authority to pursue this type of case against American businesses, and has failed to publish any regulations that would give such businesses fair notice of any proposed standards for data security."[75] To this point the FTC has not published any guidance documents particularly addressing how businesses should craft protections against cybercrime in order to avoid regulation action under the unfairness prong. However, as the Third Circuit noted in *Wyndham*, the FTC issued a guidebook in 2007, *Protecting Personal Information: A Guide for Business*, which provides businesses like Wyndham a "checklist" of practices that form a "sound data security plan."[76] While the guidebook does not provide any required practice as it pertains to § 45(a), it does make a number of suggestions:

---

[70] *Id.*

[71] *Id.*

[72] Grant Gross, *Court: FTC Can Bring Down the Hammer on Companies with Sloppy Cybersecurity*, PC WORLD (Aug. 24, 2015), http://www.pcworld.com/article/2974771/appeals-court-denies-challenge-to-ftcs-cybersecurity-enforcement.html.

[73] *Company Overview of HyTrust, Inc.*, BLOOMBERG, http://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapId=51793323.

[74] Aaron Boyd, *Should FTC Regulate Commercial Cybersecurity?*, FED. TIMES (Aug. 25, 2015), http://www.federaltimes.com/story/government/cybersecurity/2015/08/25/ftc-wyndham/32331697/.

[75] Higgins, *supra* note 67 (Statement by Michael Valentino, Vice President of Marketing and Communications for Wyndham); *see also* Sophia Pearson, *Wyndham Must Face Hacker Suit as Court Upholds FTC Power*, BLOOMBERG TECH. (Aug. 24, 2015), http://www.bloomberg.com/news/articles/2015-08-24/wyndham-must-face-ftc-suit-for-failing-to-stop-russian-hackers.

[76] FTC v. Wyndham Worldwide Corp, 799 F.3d 236, 256 (3d Cir. 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136__protecting-personal-information.pdf.

- Identify all connections to the computers where you store sensitive information.
- Encrypt sensitive information that you send to third parties over public networks (like the internet), and consider encrypting sensitive information that is stored on your computer network or on disks or portable storage devices used by your employees.
- When you receive or transmit credit card information or other sensitive financial data, use Secure Sockets Layer (SSL) or another secure connection that protects the information in transit.
- Use firewall to protect your computer from hacker attacks while it is connected to the internet . . . A properly configured firewall makes it tougher for hackers to locate your computer and get into your program and files.
- Control access to sensitive information by requiring that employees use "strong" passwords.
- To detect breaches when they occur, consider using an intrusion detection system. To be effective, it must be updated frequently to address new types of hacking.[77]

Regardless, according to Wyndham this decision pushes the limits too far, allowing the FTC "to regulate the locks on hotel room doors."[78] And as the *Wyndham* court noted, had the hotel followed some of these items from the checklist, it "could certainly have helped Wyndham determine in advance that its conduct might not survive the cost-benefit analysis."[79]

Michael Daugherty, CEO of LabMD, was in the same camp as Wyndham and has been incredibly critical of the FTC, having fought actions against the FTC that have crippled his company and forced massive rounds of layoffs.[80] LabMD is currently under fire from the FTC as it faces allegations that the company failed to reasonably protect the security of consumers' personal data, including a mixture of medical information.[81] According to the FTC complaint, LabMD collectively exposed 10,000 consumers in two separate incidents after billing information from over 9,000 consumers was found on a file-sharing network, and documents containing sensitive personal

---

[77] *Id.*
[78] *See* Pearson, *supra* note 75.
[79] *Wyndham*, 799 F.3d at 257.
[80] Boyd, *supra* note 74.
[81] *See In re LabMD*, 2015 WL 5304118 (F.T.C. 2015).

information of at least 500 consumers were found in the hands of identity thieves.[82] Nonetheless, to Daugherty the "FTC wants to become the number one self-appointed cybersecurity regulater; [and in the process the] FTC is creating common law [around cybersecurity]—get[ting] the consent decrees; build[ing] precedent; avoid[ing] the courts; mislead[ing] and stonewall[ing] congress [sic]; and play[ing] hero to the press."[83]

Even with the guidebook in place, these contentions from Daugherty and Wyndham raise relevant concerns. FTC Commissioner Terrell McSweeny admitted that the FTC was making decisions about what constitutes strong cybersecurity for the private sector despite having commissioners who are not particularly educated in what constitute strong cybersecurity measures.[84] However, McSweeny did note that the FTC relies heavily on the expertise of individuals, like Ashkan Soltani, the FTC's chief technologist.[85] Moreover, McSweeny urged individuals to get involved to help shape the regulatory policy given the uncertainty in the field.[86]

IV. HOW OTHER COMMON LAW COUNTRIES HANDLE CYBERSECURITY

The United States is not alone in facing substantial costs and threats from cyber-attacks. The United Kingdom also saw an increase from $5.93 million last year to $6.32 this year.[87] Australia saw a slight decrease from $3.99 million to $3.47 million,[88] but this is still a sizeable loss when the costs to businesses and consumers are considered. The staggering amount of damage stemming from cybersecurity breaches suggests the imminent need for regulatory oversight in all affected countries. The threats are serious and are of increasing concern to Australia's public and private sector. "Concerns about cyber risk have become the biggest concern for Australian insurance companies, jumping from 19th place four years ago to the top ranking in 2005. And it looks like the industry is bracing for sustained attack by cyber criminals."[89]

---

[82] *Id.*
[83] Boyd, *supra* note 74.
[84] *Id.*
[85] *Id.*
[86] *Id.*
[87] *See* Ponemon Institute, *supra* note 1.
[88] *Id.*
[89] Simon Thomsen, *Cyber security is now the biggest risk worrying Australian insurers*, BUS. INSIDER AUSTRALIA (Aug. 31, 2015), http://www.businessinsider.com.au/cyber-security-is-now-the-biggest-risk-worrying-australian-insurers-2015-8.

A. Australia and Cybersecurity

Australia, like the United States and the United Kingdom, has both regulatory and statutory provisions in place to combat threats to cybersecurity. This section outlines how Australia uses government initiatives, regulatory action, and the courts to hold businesses accountable for unfair business practices resulting in cybersecurity breaches. The section concludes with an Australian case study as a basis for comparing the *Wyndham* decision and the effects that the cybersecurity breaches have on both the businesses in Australia as well as the consumers.

1. The Australian Approach

In 2009, the Australian government released a "Cyber Security Strategy" in response to the Prime Minister's indication that the issue of cybersecurity is "now one of Australia's top tier national security priorities."[90] Notably, Australia's plan regarding cybersecurity seems to be more focused on education, rather than regulation.[91]

In order to meet these policy goals, the Australian government started two mutually supportive organizations: Australian Computer Emergency Response Team (CERT) and the Cyber Security Operations Centre (CSOC).[92] Australia's CERT is designed to "be the national coordination point within the Australian Government for the provision of cyber security information and advice for the Australian community and be the official point of contact in the expanding global community of national CERTs to support more effective international cooperation."[93] The CSOC "provides the Australian Government with all-source cyber situational awareness and an enhanced ability to facilitate operational responses to cybersecurity events of national importance," and "will identify and analyse sophisticated cyber

---

[90] Australian Government, CYBER SECURITY STRATEGY, at v (2009), https://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf.

[91] *See id.* ("While the Australian Government's cyber security policy is primarily concerned with the availability, integrity and confidentiality of Australia's ICT, it must be coordinated with those of other related policies and programs such as cyber *safety* which is focused on helping to protect individuals, especially children, from exposure to illegal and offensive content, cyber-bullying, stalking, and grooming online for the purposes of sexual exploitation.").

[92] *Id.* at vii.

[93] *Id.*

attacks, and assist in responses to cyber events across government and critical private sector systems and infrastructure."[94]

In March 2014, the Australian government issued a set of consolidated principles called the Australian Privacy Principals (APPs) that govern privacy and data protection throughout the country and significantly enhance regulatory protection and enforcement through the Office of the Australian Information Commissioner (OAIC).[95] Notably, the APPs allow the Information Commissioner to "assess whether personal information is being handled in accordance with the APPs or relevant legislation," and, if not, to grant the OAIC "the ability to apply the federal Magistrates Court to seek a civil penalty where an individual or company has breached a civil penalty provision of the privacy legislation."[96]

Under the watch of Australian Prudential Regulatory Authority (APRA),[97] "a business must have clear accountability and communication strategies to limit the effect of data breaches."[98] In the event of a breach, APRA expects that businesses will notify the Authority of any major security incidents.[99] Even companies that fall outside the government's reach under the APPs—companies that have licenses with the Australian Financial Services but that are not regulated by the APRA—must still have "adequate technological resources to provide financial services covered by the license and adequate risk management systems."[100]

Scholars on the subject think that organizations that allow for large breaches may face charges outside the APPs. "Current common law and statutory duties imposed on directors in Australia may . . . be interpreted to apply to data breaches in certain circumstances. Directors should give particular regard to their duties of continuous disclosure and the duty of care

---

[94] *Id.*

[95] The OAIC is an independent agency acting as the national data protection authority in Australia. *See Australian Information Commissioner Act 2010*, Act No. 62 *available as amended in 2014 at* https://www.comlaw.gov.au/Details/C2014C00382.

[96] Alec Christie & Jacques Jacobs, *The Regulatory and Legal Risks of Cyber Crime*, AUSTRALIAN INSTITUTE OF COMPANY DIRECTORS (June 1, 2014), http://www.companydirectors.com.au/director-resource-centre/publications/company-director-magazine/2014-back-editions/june/opinion-the-regulatory-and-legal-risks-of-cyber-crime.

[97] "A prudential regulator of banks, insurance companies and superannuation funds, credit unions, buildings societies and friendly societies." "The Australian Prudential Regulation Authority (APRA) oversees bank, credit unions, building societies, general insurance and reinsurance companies, life insurance, private health insurance, friendly societies and most members of the superannuation industry." Australian Prudential Regulation Authority, http://apra.gov.au/Pages/default.aspx (last visited Mar. 28, 2017).

[98] Christie & Jacobs, *supra* note 96.

[99] *Id.*

[100] *Id.* (internal quotations omitted).

and diligence under the *Corporations Act*."[101] This would include monitoring and reviewing a company's risk management and data security policies.[102] The legislative framework in Australia allows the Commissioner to "commence an investigation without a complaint,"[103] allowing broad coverage capabilities to the regulatory body.

Those charged with violating the provision may face civil penalty fines "[five] times the amount of the pecuniary penalty specified for the civil penalty provision" or "the amount of the pecuniary penalty specified for the civil penalty provision."[104] Moreover, under Section 98 of the Privacy Act, the Commissioner may apply to the Federal Courts for an injunction against the company in violation.[105] Each civil penalty provision specifies a maximum penalty for contravention of that provision. The penalty is expressed in terms of "penalty units." The value of a penalty as of March 2015 is $180 per unit.[106] According to the Privacy Act, fines may range anywhere from 500 penalty units, for low-end offenders, to 2,000 penalty units for serious or repeated violations of the Act.[107] One drawback to the penalty system used by Australia is that the fines are not used to compensate individuals who have been adversely affected by the violation.[108]

Australia also has a regulatory body in place to address issues related to cybercrime. This regulatory body, the Australian Competition and Consumer Commission (ACCC), is analogous to the FTC in many respects. The ACCC "is an independent Commonwealth statutory authority whose role is to enforce the *Competition and Consumer Act 2010* and a range of additional legislation, promoting competition, fair trading and regulating national infrastructure for the benefit of all Australians."[109] Like the FTC, the ACCC is collectively referred to as "the Commission" and has decision making authority; issues handled by the ACCC may also result in litigation. Where legal action is taken, the ACCC "is more likely to proceed to litigation in circumstances where the conduct is particularly egregious

---

[101] *Id.*

[102] *Id.*

[103] Timothy Pilgrim, *Privacy Regulatory Action Policy*, OFFICE OF THE AUSTRALIAN INFORMATION COMMISSION (June 2015), https://www.oaic.gov.au/resources/about-us/our-regulatory-approach/privacy-regulatory-action-policy.pdf.

[104] *Australian Privacy Act 1998*, pt VIB div 2s 80W para. 5, https://www.comlaw.gov.au/Series/C2004A03712.

[105] *Id.*

[106] *Crimes Act of 1914* (Cth)s 4AA (Austl.), http://www.austlii.edu.au/au/legis/cth/consol_act/ca191482/.

[107] Privacy Act, *supra* note 104.

[108] Pilgrim, *supra* note 103.

[109] Australian Competition and Consumer Commission, *About the ACCC*, https://www.accc.gov.au/about-us/australian-competition-consumer-commission/about-the-accc.

(having regard to the priority factors), where there is reason to be concerned about future behaviour or where the party involved is unwilling to provide a satisfactory resolution."[110]

In terms of protections to consumers, the ACCC relies heavily on Schedule II of the Competition and Consumer Act 2010 which is commonly referred to as the Australian Consumer Law (ACL).[111] Under Section 18 of the ACL, the ACCC may have similar unfairness powers since Section 18 allows regulation for statements that are "misleading or deceptive" or are "likely to mislead or deceive."[112]

But other sections provide additional authority to the ACCC: section 19(1)(b) applies to false or misleading representations that services are of a particular standard; section 34 applies to misleading conduct as to the nature, characteristics, or suitability for purpose of service; section 60 guarantees that services will be rendered with due care and skill, and section 61 guarantees that services will be reasonably fit for their intended purpose.[113]

Nonetheless, the ACCC has not yet utilized a litigation route to enforce these provisions. However, United States businesses that are critical of the FTC for not providing any sort of guidance or recommendations regarding cybersecurity, like LabMD and Wyndham, would not be able to make the same arguments in Australia. A variety of Australian agencies, in particular the Australian Signals Directorate, have published a number of cybersecurity guidance and recommendation measures.[114] For example, the Directorate suggests that businesses develop or utilize a variety of tools to detect breaches, including anomaly detection systems, intrusion detection systems, log analysis, network and host IDSs, and system integrity verification.[115]

---

[110] Australian Competition and Consumer Commission, *Compliance & enforcement policy*, https://www.accc.gov.au/about-us/australian-competition-consumer-commission/compliance-enforcement-policy.

[111] Competition and Consumer Act 2010 Schedule 2 (Austl.), http://www.austlii.edu.au/au/legis/cth/consol_act/caca2010265/sch2.html.

[112] *Id.*

[113] Sean Field, *Cybersecurity and the Australian Consumer Law – lessons from the US*, MADDOCKS (Sept. 9, 2015), https://www.maddocks.com.au/reading-room/cybersecurity-australian-consumer-law-lessons-america-2/.

[114] *Id.*

[115] *See* Australian Government, Department of Defense, *2015 Australian Government Information Security Manual: Controls*, http://www.asd.gov.au/publications/Information_Security_Manual_2015_Controls.pdf.

2. Case Study: Regulatory Action Against Telstra

Australia's regulatory bodies have used methods to hold Australian businesses accountable for actions very similar to those in *Wyndham*, an administrative penalty against Australian telecommunication carrier Telstra is illustrative of that point. In November 2013, Chris Chapman, Chair of the Australian Communications and Media Authority (ACMA) issued an infringement notice[116] against Telstra under Section 572E of the Telecommunications Act 1997.[117] The ACMA issued the notice following an annual compliance check of the Customer Service Guarantee benchmarks.[118] These benchmarks provide safeguards for fixed-line telephone service customers for connecting telephone service, repairing a service difficulty, and attending appointments set by customers of the company.[119] Of the nine required benchmarks, Telstra met only seven.[120] It does not appear that Telstra took the regulatory action seriously, however, because the agency found that "information of 15,775 Telstra customers from 2009 and earlier was accessible on the internet. This included the information of 1,257 active silent line customers."[121]

On May 24, 2013, the Australian Privacy Commissioner, Timothy Pilgrim, opened an investigation into Telstra.[122] The investigation focused on whether Telstra "took reasonable steps to protect customer information from misuse, loss, unauthorised access, modification or disclosure."[123] In the end, the Commission made three findings: "[Telstra] failed to take 'reasonable' steps to ensure the security of the personal information it held; failed to destroy or permanently de-identify that information; and that it

---

[116] Chris Chapman, Chair, Australian Communications and Media Authority, *Infringement Notice: Telstra 2013-001* (Nov. 27, 2013), http://www.acma.gov.au/~/media/Networks/Formal%20warnings/pdf/Telstra%20infringement%20notice%20CSG%20Nov%202013.pdf.

[117] Telecommunications Act 1997, § 572E(1) (Austl.) ("If an authorised infringement notice officer has reasonable grounds to believe that a person has contravened a particular civil penalty provision, the authorised infringement notice officer may give to the person an infringement notice relating to the contravention."), https://www.Comlaw.gov.au/Details/C2015C00540.

[118] *See* Telecommunications (Customer Service Guarantee) Standard 2011 (Austl.), https://www.legislation.gov.au/Details/F2011C00791.

[119] *See* Telstra Infringement Notice, *supra* note 116.

[120] *Id.*

[121] Press Release, OAIC (Mar. 11, 2014), https://www.oaic.gov.au/media-and-speeches/media-releases/telstra-breaches-privacy-of-15-775-customers.

[122] *Id.*

[123] *Id.*

disclosed personal information for a reason other than its permitted purpose."[124]

These findings provide a useful context when compared to *Wyndham* because, in both settings, the companies failed to "take reasonable steps" to keep the information secure. Moreover,

> the operator was also fined AU$10,200 for failing to comply with a previous ACMA decision on a data breach. In a December 2011 incident, Telstra was found to have leaked the names, and in some cases the addresses, of approximately 734,000 Telstra customers, along with the usernames and passwords of up to 41,000 of those customers online. The details were found to be publicly available and accessible on the internet between March 2011 and December 2011.[125]

In this way, like in *Wyndham*, both companies had previous incidents that should have alerted them to the potential for future breaches and the consequences that would arise if the companies did not act.

Given the breadth and reliance on regulatory regimes in Australia, it appears that Wyndham's actions would have resulted in fines for the hotel chain in Australia. Outwardly, Telstra complied with the privacy notice requirements,[126] which were meant to assure its customers that the information that it was securing was in fact safe. However, like Wyndham, Telstra failed to adequately meet the requirements as provided by the guidelines from the FTC and the Privacy Act in Australia. It follows that the U.S. guidelines need more teeth; if the guidelines were codified in a way like the Privacy Act, Wyndham's arguments would seemingly have no weight. Thus, the United States may need to look at how it informs and requires businesses to keep information safe in order to better protect consumers and more aggressively hold businesses accountable for unfair business practices that make consumer information privy to cyber-attacks.

---

[124] *See* Timothy Pilgrim, Australian Privacy Commission, *Telstra Corporation Limited: Own Motion Investigation Report*, OAIC (Mar. 2014), https://www.oaic.gov.au/privacy-law/commissioner-initiated-investigation-reports/telstra-omi-march-2014#conclusion; *see also* Jonathan Brandon & Dawinder Sahota, *Telstra Rapped for Leaking 16,000 Customers' Details* (Mar. 11, 2014), http://www.businesscloudnews.com/2014/03/11/telstra-rapped-for-leaking-16000-customers-details/.

[125] *Id.*

[126] *See* Telstra Privacy Statement, https://www.telstra.com.au/privacy/privacy-statement.

B. The United Kingdom and Cybersecurity

The United Kingdom also has regulatory and statutory provisions in place meant to circumvent attempts by hackers to steal consumer information and to combat various other threats to cybersecurity. This section outlines how the U.K. uses government initiatives, regulatory action, and the courts to hold businesses accountable for unfair business practices resulting in cybersecurity breaches. The section also concludes with a U.K. case study as a basis for comparing the *Wyndham* decision and the *Telstra* case study.

1. The United Kingdom's Approach

In 2011, the U.K. issued a National Cyber Security Strategy outlining a number of objectives, including making the U.K. "one of the most secure places in the world to do business in cyberspace" as well as making the "UK more resilient to cyber attack and better able to protect [its] interests in cyberspace."[127] Other important developments in this sector include the establishment of the U.K.'s National Computer Emergency Response Team (CERT-UK) to act as the central contact point for international counterparts in this field.[128] In addition to sector specific requirements, broad data breach requirements have been proposed as part of the General Data Protection Regulation (GDPR);[129] however, this regulation was proposed over three years ago and seems to suffer from many of the same political problems as are active in the United States, including lack of partisan support.[130]

Statutory regulation is already in effect in the U.K. The Data Retention and Investigatory Powers Act, enacted in 2014,[131] was designed to provide a platform for regulators to build obligations for businesses regarding cybersecurity concerns. However, in July 17, 2015, the English High Court

---

[127] United Kingdom, *Cyber Security Strategy* (Dec. 2014), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/386093/The_UK_Cyber_Security_Strategy_Report_on_Progress_and_Forward_Plans_-_De___.pdf.

[128] Warwick Ashford, *UK Finally Launches National Cyber Emergency Team*, COMPUTERWEEKLY.COM (Mar. 31, 2014), http://www.computerweekly.com/news/2240217221/UK-finally-launches-national-cyber-emergency-team.

[129] European Commission, *Protection of Personal Data* (Sept. 17, 2015), http://ec.europa.eu/justice/data-protection/index_en.htm.

[130] *See* Mark Young, *Cyber Security: UK Government Initiatives and Proposed EU Laws*, UNITED KINGDOM REPORT (May 2015), https://www.cov.com/~/media/files/corporate/publications/2015/05/cyber_security_uk_government_initiatives_and_proposed_eu_laws.pdf.

[131] Data Retention and Investigatory Powers Act 2014 (UK), http://www.legislation.gov.uk/ukpga/2014/27/pdfs/ukpga_20140027_en.pdf.

declared the Act was inconsistent with EU law, and it was therefore "disapplied."[132]

When it comes to personal protection, it appears that the common law may provide grounds for those aggrieved to seek compensation for a lack of adequate cybersecurity.

> Case law in [the U.K.] already tells us that where an equitable duty of confidence exists for confidential information, a parallel duty of care for security can co-exist, within the common law tort of negligence. The tortious duty for security wraps a legal envelope around the confidential relationship, to require the taking of security measures to help preserve the confidentiality of the information.[133]

The most sweeping protection, however, comes from the Data Protection Act 1998,[134] which developed requirements for cybersecurity regulation by U.K.'s Information Commissioner (ICO). ICO is the United Kingdom's independent regulatory authority, which was "set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals."[135] While the Act addresses six main principles,[136] its first principle relates specifically to fair and lawful practices. Specifically, the Data Protection Act states that: "Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless (a) at least one of the conditions in Schedule 2 is met, and (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met."[137] The conditions set out in Schedules 2 and 3 are referred to as "conditions for processing" by the ICO.[138] As such, unless some relevant

---

[132] Davis v. Secretary of State for the Home Department [2015] EWHC (Admin) 2092 (Eng.), https://www.judiciary.gov.uk/judgments/david-davis-and-others-v-secretary-of-state-for-the-home-department/. For an overview of the decision and implications *see also* Laura Woods, *Explaining the Ruling that Overturned the UK's Data Retention & Investigatory Powers Act*, LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE (July 17, 2015), http://blogs.lse.ac.uk/mediapolicyproject/2015/07/17/explaining-the-ruling-that-overturned-the-uks-data-retention-investigative-powers-act/.

[133] Stewart Room, *Cyber Security Law in the UK*, https://stewartroom.co.uk/featured/cyber-security-law-in-the-uk/ (last visited Mar. 28, 2017).

[134] Data Protection Act 1998, http://www.legislation.gov.uk/ukpga/1998/29/contents.

[135] *See* INFORMATION COMMISSIONER'S OFFICE, https://ico.org.uk (last visited Dec. 17, 2016).

[136] *Processing Personal Data Fairly and Lawfully (Principle 1)*, ICO, https://ico.org.uk/for-organisations/guide-to-data-protection/principle-1-fair-and-lawful/ (last visited Mar. 28, 2017).

[137] Data Protection Act Schedule 1, Part 1.

[138] *The Conditions for Processing*, ICO, https://ico.org.uk/for-organisations/guide-to-data-protection/conditions-for-processing/ (last visited Mar. 28, 2017).

exemption applies, at least one of the following conditions must be met by all organizations in the United Kingdom that process personal data:

- The individual whom the personal data is about has consented to the processing.
- The processing is necessary:
  - in relation to a contract which the individual has entered into; or
  - because the individual has asked for something to be done so they can enter into a contract.
- The processing is necessary because of a legal obligation that applies to you (except an obligation imposed by a contract).
- The processing is necessary to protect the individual's "vital interests". This condition only applies in cases of life or death, such as where an individual's medical history is disclosed to a hospital's A&E department treating them after a serious road accident.
- The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions
- The processing is in accordance with the "legitimate interests" condition.[139]

These are more than just suggestions—in order to ensure that organizations comply with these requirements, the Act specifically mandates that each organization submit to the register a record outlining exactly what type of information is being stored, how they are using the data, and the details of how the organization intends to maintain safety and security of the data.[140] The Act separates data into two categories: personal and sensitive data. Personal data includes information about names, addresses, medical information, and banking details.[141] Sensitive data, on the other hand, includes information that is about racial or ethnic identity, political or religious affiliation, health, sex, or criminal record.[142] The difference in the

---

[139] *Id.*

[140] See the list of six requirements at *Data Protection Act: Registration with the Information Commissioner*, GCSE BITESIZE, http://www.bbc.co.uk/schools/gcsebitesize/ict/le gal/0datapro tectionactrev3.shtml (last visited Mar. 28, 2017).

[141] *Data Protection Act: Types of Personal Data*, GCSE BITESIZE, http://www.bbc.co.uk/sc hools/gcsebitesize/ict/legal/0dataprotectionactrev4.shtml (last visited Mar. 28, 2017).

[142] *Id.*

type of data relates to the amount of safeguards that are required, and notably, there are fewer safeguards for personal data.[143]

What makes the United Kingdom's system unique is that it offers a personal right of action through the ICO. A person who has their data processed by an organization has the right to: (1) view the data an organization holds on them (for a fee); (2) request information be corrected if incorrect; (3) require that the data not be used in any way that is potentially harmful or distressing; and (4) require that their data not be used for direct marketing purposes.[144]

The biggest threat comes by way of the ICO's ability to hold organizations accountable through a number of mediums. The main options include:

- serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;
- issue undertakings committing an organisations to a particular course of action in order to improve its compliance;
- serve enforcement notices and 'stop now' orders where there has been a breach, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- conduct consensual assessments (audits) to check organisations are complying;
- serve assessment notices to conduct compulsory audits to assess whether organisations processing of personal data follows good practice;
- issue monetary penalty notices, requiring organisations to pay up to £500,000[145] for serious breaches of the Data Protection Act occurring on or after 6 April 2010
- prosecute those who commit criminal offences under the Act; and
- report to Parliament on issues of concern.[146]

---

[143] *Id.*

[144] *See* BBC, *supra* note 140.

[145] The equivalent of over $750,000.

[146] Information Commissioner's Office, *Taking Action – data protection*, https://ico.org.uk/about-the-ico/what-we-do/taking-action-data-protection/.

According to the ICO,

> [i]t is clear from the wording of [ ] the Act that a monetary penalty notice will only be appropriate in the most serious situations. Therefore in such cases the monetary penalty must be sufficiently meaningful to act both as a sanction and also as a deterrent to prevent non-compliance of similar seriousness in the future by the contravening person and by others.[147]

The Act goes one step further; the ICO has the ability to hold directors of offending companies personally liable in certain circumstances, putting serious pressure on companies to comply with the Act's sweeping language.[148]

The ICO has included a number of examples of ways in which an organization would be in serious contravention of the Act, warranting a fine. One example given "failure by a data controller to take adequate security measures (use of encrypted files and devices, operational procedures, guidance etc.) resulting in the loss of a compact disc holding person data."[149] The ICO made it clear that it was willing to use this power when it recently fined the Pregnancy Advice Service £200,000[150] for its failure to secure a website.[151]

2. Case Studies: To Settle, Win, or Pay Up?

Cybersecurity regulation in the U.K. seems to be in a similar position as in the United States. At first, it appeared that some of the U.K. businesses might resist the regulatory regime, but in the end most of those cases have settled. For instance, Sony[152] and Marks & Spencer[153] both dropped their

---

[147] Information Commissioner's Office, *Information Commissioner's Guidance About the Issue of Monetary Penalties Prepared and Issued Under Section 55c (1) of the Data Protection Act 1998*, at 6 (Dec. 2015), https://ico.org.uk/media/for-organisations/documents/1043720/ico-guidance-on-monetary-penalties.pdf.

[148] Alison Deighton, *Directors to Be Personally Liable for Marketing Breaches*, TLT SOLICITORS (Nov. 22, 2016), http://www.titsolicitors.com/insights-and-events/insight/directors-to-be-personally-liable-for-nuisane.calls/.

[149] *Id.* at 10.

[150] Approximately 300,000 U.S. Dollars.

[151] Information Commissioner's Office, *supra* note 147.

[152] Out-Law, *ICO Fines Sony £250,000 over Security Failings that Exposed 'Millions' of UK Customers' Personal Data* (Jan. 24, 2013), http://www.out-law.com/en/articles/2013/january/ico-fines-sony-250000-over-security-failings-that-exposed-millions-of-uk-customers-personal-data/.

respective cases and settled. This kind of response mimics that in the United States, even with the recent *Wyndham* decision. As previously noted, the FTC has settled over fifty cases with businesses regarding cybersecurity issues.[154] This idea is illustrative of a few aspects of both regulatory regimes: first, that it might just be cheaper to pay the regulating body when you have a breach than it is to address the heart of the problem; and alternatively, this may mean the regulation is working and businesses will eventually comply.

Interestingly, one business has successfully been able to appeal a decision by the ICO. A U.K. tribunal in August 2013 decided that the ICO "was wrong to impose a £250,000 fine on [the] Scottish Borders Council."[155] The case centers around an "incident where pension records of former Council employees were discovered overflowing from recycling bins outside a local supermarket."[156] In the end, the Tribunal determined that while the infraction was serious, it was "not . . . likely to cause substantial damage or substantial distress," a requirement for imposing a penalty.[157] What is important to consider in this case is the regulations in the U.K.; namely, the self-reporting requirements. Should businesses be required to report a potential violation? And if they fail to report, should they be treated more harshly under the eyes of the regulation? The Tribunal's opinion is illustrative:

> The Tribunal decision includes a number of interesting comments under the heading "Unfinished Business." In particular, it suggests consideration should be given as to whether self-reporting is a relevant factor in the exercise of the penalty discretion — in the UK it is not mandatory to report a breach, but ICO decision notices indicate that a failure to self-report is regarded as an aggravating factor when determining the penalty it imposes.[158]

---

[153] Tom Young, *M&S Appeal Dropped as it Encrypts Laptops*, COMPUTING (Sept. 25, 2008), http://www.computing.co.uk/ctg/news/1829583/m-s-appeal-dropped-encrypts-laptops.

[154] *See* Pearson, *supra* note 5.

[155] Mac Macmillan, *UK Council Successfully Appeals ICO Fine Arising from Processor Breach*, CHRON. DATA PROTECTION (Sept. 4, 2013), http://www.hldataprotection.com/2013/09/articles/employment-privacy/local-council-successfully-appeals-against-ico-fine/.

[156] *Id.*

[157] Scottish Borders Council v. Information Commissioner, EA/2012/0212, http://www.informationtribunal.gov.uk/DBFiles/Decision/i1068/Scottish%20Borders%20Council%20EA.2012.0212%20%28210813%29%20Preliminary%20Decision.pdf.

[158] *See* Macmillan, *supra* note 155.

What should happen if a business unsuccessfully appeals? A U.K. business, Reactive Media recently found out. The ICO served Reactive Media with £50,000 fine for a breach where "more than 600 complaints concerning unsolicited marketing phone calls made by the company were received by the ICO."[159] Reactive Media "found itself facing a 50% increase in the fine it was attempting to overturn after an appeal."[160] On appeal, Reactive argued that "there was no evidence that its communications had caused 'substantial damage or distress', and that as it 'offered a service to the public, it had a right to trade, [and] it was trading well in an area of high unemployment.' "[161] However, the Tribunal disagreed, feeling that the ICO was able to accurately determine the Reactive's finances, so it unanimously held that a £75,000 fine was more appropriate.[162]

This 2015 decision may suggest that the tides are changing in the U.K. Historically, ICO decisions like these are rarely upheld, so this decision could prove to be the impetus required for companies to become more compliant with their privacy requirements. The ICO has already hinted that it will start to issue more fines to deter unsolicited marketing activities; organizations should therefore be aware that privacy-related incidents will no longer be tolerated.[163] The same could be said for the Third Circuit's decision in *Wyndham*. Courts have been reluctant to allow businesses to circumvent the FTC's determinations, and instead have held them accountable for situations where they have participated in unfair business practices. While it seems unlikely that a U.S. court would increase the fines imposed by the FTC, a feature in the statutes that impose additional fines on unsuccessful appeals may be used as an additional deterrent, thus making businesses more likely to comply with cybersecurity regulation.

C. Are These Efforts Working?

In the face of rising threats to cybersecurity, naturally the question arises: are these efforts of the other common law countries working? The regulations and framework implemented in the United Kingdom appear to be a step in the right direction, and the U.K. government is continuing to invest in ways to address cyber risks. In a recent speech at the GCH intelligence

---

[159] Cynthia O'Donoghue, Kate Brimsted & Chantelle Taylor, *Reactive Media Fine Increased on Appeal by UK Information Rights Tribunal*, REED SMITH TECHNOLOGY LAW DISPATCH (July 10, 2015), http://www.technologylawdispatch.com/2015/07/privacy-data-protection/reactiv-media-fine-increased-on-appeal-by-uk-information-rights-tribunal/.

[160] *Id.*

[161] *Id.*

[162] *Id.*

[163] *See* Deighton *supra* note 148.

agency, Chancellor George Osborne named the technology section as an area of priority for the government.[164] "Osborne announced a plan to nearly double spending on cyber security investment[s], bring[ing] the total to more than £3.2 billion,"[165] maintaining that the United Kingdom is dedicated to developing "a bold, comprehensive [program] that will give Britain the next generation of cyber security, and make Britain one of the safest places to do business [online]."[166]

Despite these efforts, the respective governments are mindful of the numbers. Recall, the United Kingdom saw an increase in lost revenues from $5.93 million last year to $6.32 this year as a result of cybersecurity threats.[167] Australia experienced a slight decrease from $3.99 million to $3.47 million.[168] "[J]ust twenty-three Australian businesses were surveyed," however and this relatively small sample size may explain why Australia fared better than its common law counterparts.[169]

The attack really needs to be on two fronts. As the Ponemon study articulates, the various costs associated with cybercrime can be "moderated by the use of security intelligence systems (including SIEM). Findings suggest [that] companies using security intelligence technologies were more efficient in detecting and containing cyber-attacks. As a result, these companies enjoyed an average cost savings of $1.9 million when compared to companies not deploying security intelligence technologies."[170] If Ponemon is right, this severely undercuts any argument by United States companies who see the FTC's actions against Wyndham as a serious threat to American business.

V. HOW TO RESPOND TO THE INCREASED RISK OF CYBERATTACKS

A. Is the Current United States Model Enough?

While the FTC may have support from the courts, it does not appear that the current model will be able to keep up with the increasing threats to

---

[164] Natasha Lomas, *U.K. Gov't to Invest $250M in Cyber Security Start Up to Help Spooks*, TECH CRUNCH (Nov. 18, 2015), http://techcrunch.com/2015/11/18/uk-gov-to-invest-in-security-startups/.

[165] Over 4.8 billion U.S. Dollars.

[166] *See* Lomas, *supra* note 164.

[167] Ponemon Institute, *supra* note 1.

[168] *Id.*

[169] Beverly Head, *The True Cost of a Cyber Security Breach in Australia*, COMPUTER WKLY. (Oct. 2015), http://www.computerweekly.com/news/4500254729/The-true-cost-of-a-cyber-security-breach-in-Australia.

[170] Ponemon Institute, *supra* note 1, at 19.

consumer information. The staggering numbers from the Ponemon Institute study, coupled with the countless articles about cyber threats flashing across the news headlines suggests the United States is in need of a system that draws on all of the strengths of these three countries' systems.

Foremost, the United States needs to continue to try to educate businesses and consumers on how to protect information. Consider Australia's plan regarding cybersecurity, which seems to be heavily focused on education.[171] While Australia's system may be too focused on the education aspect, informing consumers and businesses about ways to avoid attacks could reduce attackers' ability to steal information. While this should not be the centerpiece of the American system, it surely should be a tool that the FTC can use to reduce the number of attacks each year.

Second, the FTC, or even the Consumer Financial Protection Bureau, could benefit from legislation that has more grit. While there is currently proposed legislation[172] regarding cybersecurity, it is directed at an issue altogether different than the one principally discussed in this Note. Rather, the proposed legislation seems to target the sharing of information with other countries in order to strengthen the ability of governments to go after attackers.[173]

Improving information security should fundamentally involve securing information, yet all the current proposals involve *greater* information sharing with intelligence agencies. "Why are the same agencies that have been shown to be active in undermining the information security of private firms . . . and all of their customers . . . as a consequence of these actions, being tasked with better securing our information?"[174]

While the United States, the U.K. and Australia would benefit from this type of information exchange, it would fail to address the underlying systemic issue. Arguably, the FTC has the authority to go after these businesses like it did in *Wyndham*, but more detailed legislation may remove some of the obstacles in place against the FTC to better enable the Commission to get businesses to implement best practices when it comes to cybersecurity protection. While the guidelines provide a starting base, they lack the enforcement strength needed to hold businesses accountable when they fail to meet the guidelines.

---

[171] *See* Cyber Security Strategy 2009, *supra* note 90, at 6.

[172] See the proposed legislation discussed *supra* note 30.

[173] See the proposed legislation discussed *supra* note 30.

[174] Benjamin Dean, *Why Companies Have Little Incentive to Invest in Cybersecurity*, THE CONVERSATION (Mar. 4, 2015), http://theconversation.com/why-companies-have-little-incentive-to-invest-in-cybersecurity-37570.

Finally, the FTC needs to more actively pursue businesses who fail to have effective cybersecurity protections. This serves a number of functions: first, it will likely lead to more policy opinions by the FTC which would guide businesses on what is expected. While the most effective means would be better served from avoiding a potential *ad hoc* determination of what is required from businesses. Second, the increased pressure by the regulatory arm might incentivize businesses to find ways to keep consumer information safe instead of being met with fines. Finally, the FTC will need to continue to monitor and work with individuals and businesses who specialize in keeping information safe from hackers. As technology continues to evolve, the FTC will have to continue to meet the growing demands and threats. By actively and continually monitoring cybersecurity, the FTC could potentially increase the use of better cybersecurity protections, thereby reducing the large sums spent each year on cyber-related attacks.

B. Cyber Insurance—Buyer Beware

Are there ways that businesses can advance these goals? While the government attempts to create better security practices online, some businesses have begun to invest in cyber insurance. In places like the United Kingdom, directors can be personally liable.[175] Insurance in the U.K. is likely attractive for two reasons: first, it mitigates the costs to the company (and potentially to directors) and second, it a company's reputation is improved when it provides assurance to its customers.

While there are many benefits, however, insurance has its drawbacks. Particularly in the U.K. where directors may be held personally liable, having insurance may act as a disincentive for companies to address the roots of their problems.[176] Instead of finding better ways to monitor and secure information, companies are spreading the cost to the consumers while failing to address the reasons why insurance is needed. Moreover, very little historical actuarial data exists, so when it comes to pricing premiums for companies, serious challenges exist for finding appropriate premium costs.[177]

Security professionals are starting to warn businesses not to rely on cybersecurity insurance to address the increased risks of cyber-attacks.

---

[175] For more about cyber insurance and an example of a reaction see Elliot Shear, *Cybersecurity-"The Directors of 98% of UK Companies Are in Breach of Their Statutory Duties,"* W LEGAL (Feb. 7, 2017, http://wlegal.co.uk/cybersecurity-the-directors-of-uk-companies/.

[176] Tim Holman, *Security Think Tank: Cyber Insurance – Buyers Beware*, COMPUTER WKLY. (Oct. 2013), http://www.computerweekly.com/opinion/Security-Think-Tank-Cyber-insurance-buyers-beware.

[177] *Id.*

Notably, one of the largest insurance providers said that "cyber attacks are now so dangerous to global businesses that governments should step in to cover the risks."[178] Arguably, directors have very little incentive to invest in cybersecurity, particularly in the United States because no such current risks fall upon them.

There are also some great misconceptions surrounding the actual coverage that current insurance provides to the companies. Namely, many individuals think that the policies include insurance for data theft and loss. "In the UK, at least, data is not considered a tangible asset that one can steal, hence [there is] computer misuse and data protection law to cover these eventualities."[179] This creates a greater uncertainty as to whether an individual should seek out personal data insurance coverage, or whether the coverage and policies purchased by customers will in fact be able to handle the potentially large payouts that would result from any sort of substantial breach.

VI. CONCLUSION

In the end, these governments need to find ways to make the idea of cybersecurity investment desirable. Recently, President Barack Obama announced that he was seeking $14 billion to tackle the issue, but this does not address the heart of the issue.[180] Rather than creating various incentives for businesses to invest in stronger security measures, the United States (as well as Australia and the United Kingdom) is introducing proposals for more information sharing with intelligence agencies.[181] If these countries want to limit access to consumer information and hold businesses accountable for unfair or deceptive practices which enable to hackers to take this sensitive information, then the attack needs to be on more fronts. Countries like the U.K., which name the technology sector an area of priority for the government[182] without implementing laws and regulations that force businesses to adopt better practices, are failing to address critical issues.

The government that is best able to educate consumers and businesses, create incentives for businesses to comply with effective statutory and regulatory action, and continue to pressure businesses to meet compliance standards will likely see the greatest defense to cyber-attacks. The decision

---

[178] *Id.*
[179] *Id.*
[180] AFCEA, *The Need to Shave: The U.S. Intelligence Community and Law Enforcement* (Apr. 2007), http://www.afcea.org/mission/inel/documents/SpringIntel07whitepaper_000.pdf.
[181] *Id.*
[182] Lomas, *supra* note 164.

in *Wyndham* may help push that agenda because it signifies to businesses that the FTC has the support of the courts in enforcing these types of decisions. This demonstrates the need for a full and comprehensive attack by the government: the legislative, judicial, and executive need a comprehensive interconnected plan if meaningful change is to occur in this sector.