SYRACUSE JOURNAL OF
SCIENCE & TECHNOLOGY LAW

VOLUME 33 2016-2017

TABLE OF CONTENTS

Syracuse Journal of Science & Technology Law

Volume 33 2016-2017

2016 - 2017 Editorial Staff

Cyber Security and the Grid: We'll Leave the Lights on for You (If We Can)[1]

Joseph Abrenio, joel gridley, Christopher Folk

Overview

The U.S. power grid plays a vital role in the nation's health and welfare. The U.S. relies upon a consistent and continuous supply of electrical power to fuel transportation, power its industries, and sustain its healthcare system. Yet, this critical asset is often taken for granted, even though just a minor disruption of the vast network of our power grids could have devastating impacts. The loss of power—in even a small, isolated area—can leave homes without heating or cooling, interrupt local businesses, and down traffic control devices. A regional or national disruption could bring commerce and manufacturing operations to a halt, or even worse, disable critical care and surgical facilities. The ripple effects could mean catastrophic economic loss or loss-of-life. Furthermore, the short-term and long-term national security implications that would arise from an attack on our critical infrastructure would be significant.

The goal of this white paper is to provide a deeper understanding of the role of the grid in our critical infrastructure paradigm; the current grid regulatory scheme; and the technical and non-technical cyber threats facing the grid, including legal liability for operators.

As an introduction, we provide an overview of critical infrastructure and specifically, the power grid, as well as technical and non-technical issues facing the grid. Next, we offer an overview of the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards that provide a regulatory framework.

---

1 This article was previously published in the Journal on Terrorism and Security Analysis 12th Edition (Spring 2017).
The Journal on Terrorism and Security Analysis, Syracuse University (12 Ed., Mar. 2017),

Finally, we address best practices, risk mitigation, risk transfer methods, and security risk assessments in the context of operations, IT operations, and compliance.

Critical Infrastructure

The electric grid is one of the most complex and critical components of infrastructure because so many other sectors are dependent upon it for their own continued operations. With the transition from mechanical devices to digital remote and control functions to manage the grid, the risks presented by bad actors have dramatically increased. Furthermore, the risks to critical infrastructure and cyber events in general have received widespread media attention in recent years. While it is beneficial to shed light on the problems, many media outlets have been quick to jump to conclusions and provide poorly-vetted accounts of cyber intrusions, which can do more harm than good by sensationalizing such news and ultimately lead to industry and consumer fatigue or even disbelief. Consider the December 2016 report, which stated that a Vermont utility was hacked and reportedly had signs related to Grizzly Steppe.[2] While this was widely reported, it was quickly revealed that the Vermont grid had not actually been infiltrated, the device in question was never connected to the grid networks, and the origin was not likely Russia[3] Consequently, security professionals must be vigilant and ensure that they properly investigate and understand the situations that may be encountered.

A. Power Grid Overview

The first local grid began operating in 1882, suppling a small group of customers in Manhattan with low-voltage electricity using direct current connections.[4] At the

2 Warner Todd Huston, *Washington Post's Fake News of Russian Vermont Power Plant Hack*, Breitbart News (Dec. 31, 2016), http://www.breitbart.com/big-government/2016/12/31/washington-posts-fake-news-russian-vermont-power-plant-hack/.

3 *Id.*

4 JS, *How Electricity Grew Up? A brief History of the Electrical Grid . . .*, Power2Switch (Oct. 25, 2012), https://power2switch.com/blog/how-electricity-grew-up-a-brief-history-of-the-electrical-grid (The Pearl Street Station in Manhattan provided service to 85 customers, powering approximately 400 lamps).

end of the 19th century, the industry largely adopted the use of alternating current (AC), which enabled electricity to be transmitted across far greater distances. This technological advancement sparked a period of utility consolidation, and by the turn of the 20th century, approximately 4,000 distinct and isolated electric utilities distributed electricity to their geographic localities.[5] This was further bolstered by the industrialization effort in a post-World War II era. Ultimately, 2,000 electric distribution utilities were grouped into three "sectional" grids that supply power to 48 states: (1) The Eastern Interconnection (typically includes those states east of the Rockies); (2) the Western Interconnection (which reaches from the Rocky Mountain states to the Pacific Ocean; and (3) the Texas interconnected system (which, as the name implies, includes Texas).[6] These sectional grids continue to exist today.

What is SCADA?

Like all industries, the power industry looked to new technologies to increase efficiency and profitability by coordinating and optimizing power transmission between and amongst interconnected grids. [7] Grid operators employed industrial control systems (ICS), and specifically, supervisory control and data acquisition (SCADA) systems, for greater energy transmission.[8] SCADA is essentially a combination of hardware and software that allows complex control and monitoring of physical industrial equipment.

While often associated with utilities, every industry leverages SCADA. In fact, the term SCADA is a generic category which implies the system from which control and monitoring is achieved. For example, car manufacturers use SCADA systems to

5 *Electricity Explained: How Electricity is Delivered to Consumers*, U.S. Energy Info. Admin., http://www.eia.gov/energy_in_brief/article/power_grid.cfm (last visited Nov. 22, 2016); *The Electricity Grid: A History*, Burn an Energy J., http://burnanenergyjournal.com/the-electricity-grid-a-history/ (last visited Dec. 27, 2016).

6 *Id.*

7 Tamilman Vijayapriya & Dwarkadas Pralhadas Kothari, *Smart Grid: An Overview*, Sci. Res. (June 7, 2011), http://file.scirp.org/pdf/SGRE20110400016_22126588.pdf.

8 *Id.*

control the machinery involved in the manufacturing process.[9] Similarly, a dam operator uses a SCADA system to measure the amount of water flow through a dam's controlled spillway, while pharmaceutical companies utilize SCADA systems to control mechanized sorting machines and conveyors in the automated packaging of drugs for delivery to distribution centers.[10]

However, the specific uses of SCADA systems are industry-driven. While certain principles, architecture, and terminology remain standard, specialization or customization from industry to industry is required. The use of ICS and SCADA was a large driver in the evolution from an analog to a digital grid, referred to as the Smart Grid.

A. Evolution of the Smart Grid

The power grid's network of mechanical, analog controls was highly inefficient in the transmission and distribution (T&D) of energy because each mechanical component introduced resistance. Multiplied over hundreds or thousands of devices, the cumulative resistance was significant. Experts estimate that traditional, non-digital controls limited the grid to approximately 60 percent of overall transmission capabilities.[11] The mechanically-controlled, analog grid was a collection of moving parts that was doomed to fail over time due to thermal breakdown or mechanical component failures.[12]

In response, grid operators began designing and implementing electronic controls and devices using solid-state superconductors, which increased electricity transmission and distribution. Just as critical, these new technologies allowed for remote control, monitoring, and modification, thereby decreasing maintenance time and further

---

9 Zenon for Automotive, CopaData (last visited Feb. 8, 2017), https://www.copadata.com/en/process-control-system/automotive/.

10 Frank R. Spellman, Dam Sector Protection and Homeland Security (Bernan Press, 2017).

11 U.S. Dep't of Energy, Enabling Modernization of the Electric Power System: Technology Assessments (2015), https://energy.gov/sites/prod/files/2015/09/f26/QTR2015-3F-Transmission-and-Distribution_1.pdf.

12 *Id.*

increasing utility profits.

As a direct result of electronic devices—and supported by the design, development, and deployment of the Internet of Things (IoT)—the modern Smart Grid was born. The Smart Grid is now capable of interacting through even basic household appliances through their embedded technologies. However, this Internet gateway possesses unintended threats, as these IoT devices are particularly susceptible to power issues.[13] Nonetheless, as our electrical infrastructure continues to age, and various components are approaching their useful end-of-life (EOL), the movement to the Smart Grid (with monitoring, analysis, control, and communication capabilities) is essential to providing reliable and consistent power transmission in the face of ever-growing needs.

For instance, one of the key Smart Grid components is demand side management, which maximizes load balancing and minimizes cascading failures.[14] Demand side management enables grid connections to distributed generation power (wind turbines, photovoltaic (solar) arrays) and fosters grid energy storage, wherein stored power is used to offset high demand periods and prevent rolling outages.

Additional Smart Grid functions include:[15]

- Efficient transmission of electricity;
- Re-generation and restoration of services in a post-power disturbance scenario;
- Demand and load balancing; and
- The integration of renewable energy sources.

The economic benefits from these new functionalities are lower operational and management costs. In addition, grid operators can leverage large-scale power

---

13 *What is Smart Grid and Why is it Important?*, Nat'l Electrical Manufacturers Ass'n, https://www.nema.org/Policy/Energy/Smartgrid/Pages/What-Is-Smart-Grid.aspx (last visited Nov. 23, 2016).

14 *Id.*

15 *What is the Smart Grid?*, SmartGrid.Gov, https://www.smartgrid.gov/the_smart_grid/smart_grid.html (last visited Nov. 23, 2016).

production and provide more consumer-driven power production, again benefitting the economic bottom line.

B. Critical Infrastructure Threats

Following the domestic terrorism event in Oklahoma City in 1995, Attorney General Janet Reno urged President Clinton to create a commission to examine U.S. vulnerability to attacks at "key facilities."[16] Consequently, President Clinton formed the Presidential Commission on Critical Infrastructure Protection (PCCIP).[17] General Robert Marsh (USAF Ret.),[18] was appointed as its Chairman. The PCCIP developed the term "critical infrastructure" to designate key U.S. facilities, and formed the "Marsh Commission" to investigate and report on threats to the nation's critical infrastructure.[19]

In 1997, the Marsh commission delivered a report (the "Marsh Report") that focused on the Internet, underscoring the fact that the country's most important functions were often routed through the Internet, and any disruption of the Internet could cause widespread outages or damage to our critical infrastructure.[20] The Marsh Report urged a coordinated effort to protect the U.S. against the prospect of nation-states creating "information war" offensive units.[21] However, the Marsh Report warned that much of the burden would fall upon the private sector, as it owned the bulk of the critical infrastructures.[22] The Marsh Report further warned that these industries would likely be reticent to invite government regulation in their industries under the guise of cyber security.[23]

---

16 Richard A. Clarke, Cyber War: The Next Threat to National Security and What to do About it 105 (2010).

17 *Id.*

18 *Id.* at 106.

19 *Id.*

20 *Id.*

21 Clarke, *supra* note 15.

22 *Id.*

23 *Id.*

C. The Wake-Up Calls: 1999 and 2003

A cyber threat to critical infrastructure was realized on June 11, 1999, when a gasoline pipeline in Washington State burst and began spilling fuel into a nearby creek.[24] The gasoline ignited, killing three people and causing extensive damage to a nearby water-treatment plant.[25]

A subsequent investigation by the U.S. National Transportation Safety Board (NTSB) determined that the root cause of this event was a software failure within the SCADA system.[26] Although there was no indication in the report that the incident was related to any malicious activity, the fact that a software failure in a SCADA system could result in palpable, physical damage underscored the fact that cyber security was a legitimate concern.[27]

In 2003, a computer malware worm named "Slammer" infiltrated and consumed computing power within power grid SCADA systems, causing the controls to become less responsive.[28] Consequently, when a tree fell in Ohio and caused a surge, the SCADA systems could not successfully prevent a cascading power loss affecting eight states and more than 50 million people.[29] This single event demonstrated that a targeted cyber-attack on the power grid coupled with a physical attack could have devastating effects.

D. The Threat Becomes Real: Cyber-Attacks on Power Grids and Critical Infrastructure

---

24 *Id.* at 97.

25 *Id.*

26 Clark, *supra* note 15, at 97.

27 This is an inference made by the author since the report did not point to malicious intent but rather a failure in a SCADA system from which physical damage resulted.

28 Paul Ducklin, *Memories of the Slammer Worm: Ten Years Later*, Naked Sec. (Jan. 27, 2013), https://nakedsecurity.sophos.com/2013/01/27/memories-of-the-slammer-worm/.

29 Clarke, *supra* note 15, at 99.

As recently as December 17, 2016, a cyber-attack directed at the Ukraine power grid left homes without power for over an hour.[30] This was reminiscent of a similar attack that occurred in December 2015, when a cyber-attack against the Ukraine power grid resulted in a loss of power for more than 225,000 citizens.[31] According to the Department of Homeland Security (DHS), this event marked the first successful cyber-attack to take a power grid offline.[32] Fortunately, the latest incident in 2016 was short-term in duration and had a narrow reach. With temperatures ranging from 15 to 30 degrees Fahrenheit, if the outage lasted longer, and occurred over a broader geographical swath, people could have died.[33]

In the summer of 2013, Iranian hackers infiltrated the control systems of a dam near New York City.[34] While this attack resulted in no known damage, the fact that the hackers were able to penetrate and gain access to these control systems was remarkable.[35] Even more concerning, experts report that Iranian attackers targeting other critical infrastructure have successfully exfiltrated highly sensitive data such as mission-critical power plant blueprints.[36]

A rising concern for U.S. officials is the combination of a kinetic and cyber-attack in a multi-phasic approach to trigger an actual invasion. For instance, Russia's

---

30 John Leyden, *Energy Firm Points to Hackers after Kiev Power Outage*, Register, http://www.theregister.co.uk/2016/12/21/ukraine_electricity_outage/ (last visited Dec. 27, 2016).

31 *Id.*

32 Dustin Volz, *U.S. Government Concludes Cyberattack caused Ukraine Power Outage*, Reuters, http://www.reuters.com/article/us-ukraine-cybersecurity-idUSKCN0VY30K (last visited Nov. 23, 2016) (The attacks on the Ukraine were purportedly initiated from remote cyber intrusions into three regional electrical power distribution companies where ICS systems were targeted and exploited).

33 Leyden, *supra* note 29.

34 *Schumer: Iranian Cyber-Attack on New York Dam was "Shot Across the Bow"*, Tower (Mar. 15, 2016, 8:09 AM), http://www.thetower.org/2090-schumer-iranian-cyber-attack-on-new-york-dam-was-shot-across-the-bow/.

35 *Id.*

36 *Id.*

alleged pre-emptive distributed denial-of-service (DDoS) attack against Georgia was used to disrupt the country's communication networks prior to the Russian army invasion.[37] This cyber event was powered with a kinetic conventional attack in the form of a physical invasion, which made for a highly-effective belligerent action.[38] The one critical distinction between Georgia and the U.S. in this instance is that Georgia was not as reliant upon technology. The cyber-attack perpetrated against Georgia caused little damage other than the loss of website accessibility—all other communication methods remained online.[39] Were such an attack directed at the U.S., the effects could be far more severe and wide-ranging, as the U.S. is much more dependent on Internet communications.

The well-known Stuxnet computer worm—reportedly designed to infiltrate Iran's Nuclear centrifuge program—is another example of a cyber incident with implications in the physical realm. The Stuxnet attack targeted command and control software and caused the centrifuges to essentially self-destruct, while also disrupting monitoring capabilities so everything appeared to be running normally.[40] This event was significant, as it was reportedly the first actual deployment of a cyber-physical attack that crossed the two realms, causing damage within each.

Using the lessons learned from these events, the National Research Council (NRC) delivered a report in 2012 in which it concluded that a coordinated terrorist attack directed at the power grid could result in a wide-scale blackout that would persist for weeks or perhaps months.[41] The NRC also theorized that if a combined kinetic and

---

37 John Markoff, *Before the Gunfire, Cyberattacks*, N.Y. Times (Aug. 12, 2008), http://www.nytimes.com/ 2008/08/13/technology/13cyber.html?_r=0.

38 *Id.*

39 *Id.*

40 Bipartisan Policy Ctr., Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat (2014), http://bipartisanpolicy.org/wp-content/uploads/sites/default/files/ Cybersecurity%20Electric%20Grid%20BPC.pdf.

41 Nat'l Acad. of Sci., Terrorism and the Electric Power Delivery System (2012), https://www.nap.edu/catalog/12050/terrorism-and-the-electric-power-delivery-system.

cyber-attack were coordinated and timed to transpire during periods of prolonged cold weather, the effect could be catastrophic.[42] Aside from the obvious economic losses, an attack of this scale could also result in thousands or hundreds of thousands of deaths due to extended exposure to extreme cold temperatures.[43]

E. Technical Cybersecurity Issues Facing the Grid

i. Esoteric Nature of SCADA systems

For the reasons discussed above, power grid SCADA systems are extremely unique and specialized. Moreover, the applications and processes that manage and direct telemetry and control communications of each SCADA system are proprietary software and are specific to the vendor which produces it. Because vendors are often responsible for designing these specialized SCADA systems, the IT Operations staff ultimately operating them may lack a comprehensive understanding of their own SCADA environment, as they are often based on proprietary software. Even when installed on typical operating systems such as Unix or Windows, the operating system itself can behave in unfamiliar ways. What would be considered standard IT procedures in any other environment (such as routine OS updates or password changes) may prove disruptive in a specialized and proprietary SCADA environment.

ii. Corporate Move to "Cloud" Environments

A recent trend, both among corporations and the vendors they employ, is moving infrastructure and services to the "cloud." Even sensitive services, such as security patches (CIP-007R2), or anti-virus software and signature updates (CIP-007R3), (which many responsible entities are dependent upon for maintaining compliance and a secure SCADA environment) are moving, or have already moved to the cloud.[44]

---

42 *Id.*

43 *Id.*

44 Kevin Parker, *SCADA Remains Relevant for Industrial Automation*, Control Engineering (Dec. 7, 2016), http://www.controleng.com/single-article/scada-remains-relevant-for-industrial-automation/5e5c4f48da a67663752ffe385047ab4a.html.

In addition to services such as weather forecasts and Outage Management Systems (OMS) directly interacting with the SCADA environment, responsible entity corporate networks are becoming increasingly dependent upon cloud-provided services, applications, and storage, and are inextricably exposed to data leakage risks.[45]

iii. Cost of Commitment, Lack of Interoperability

Choosing a SCADA system vendor is a massive commitment in time and capital expense. Furthermore, a utility is often locked into a vendor for many years as these systems have virtually no interoperability with any other equipment, other than custom interoperability designed and implemented in the initial SCADA solution.[46] Because of this lack of interoperability, if any equipment or software bundled in the solution is found to be unable to conform to compliance requirements or security best practices, there is usually very little to no opportunity to replace the equipment or software with alternatives. As a result, there is no easy upgrade when SCADA solutions become outdated. A utility is forced to develop a completely new architecture, purchase new equipment, and conduct new training for the IT Operations Staff.

iv. Undocumented "Features" in SCADA Environments

IT Operations Staff are often forced to rely upon the documentation provided by SCADA vendors to understand the operational behaviors and requirements of the environment. Unfortunately, not all behaviors and requirements are explicit, and sometimes they are only implied. Thus, IT Operations Staff who may be unfamiliar with the SCADA application, device, or process may miss or misinterpret signals.

---

45 *Integrated Distribution Management on a Cloud*, CapGemini, https://www.br.capgemini.com%2Fresource-file-access%2Fresource%2Fpdf%2Fintegrated_distribution_management_system _on_a_cloud.pdf& usg=AFQjCNHRjT8-nj6LYI_iihy71Zin_zgORw&sig2=O8jw416dOlsDPL-pHEIUfw (last visited Feb. 8, 2017).

46 SCADA solutions are generally custom-tailored to specific environments and uses. Thus, an entity that implements a SCADA solution can customize it and enable interfaces when it is implemented. Post-implementation, an entity would either need to rely on in-house expertise or use vendor resources to enable interoperability with other products.

Because SCADA solutions are proprietary products, there are few, if any, additional resources besides the vendor to turn for more documentation, explanation, or instructions. Adding to this is the sensitive nature of SCADA solutions in the utility industry. Although you can typically find all sorts of online resources regarding managing firewalls, databases, and servers, it's difficult to find such information when it comes to SCADA solutions. The "security through obscurity" paradigm typically applied in SCADA environments often produces unintended results, as operators and staff do not share critical threat information from one utility to another.

v. Updates Delayed by Shortcomings in SCADA Software

During the lifecycle of any computing environment, security patches and operational updates are common and expected. However, vendors are routinely slow in producing timely SCADA security software patching, leaving SCADA systems dangerously vulnerable to even know cyber weaknesses. These vulnerabilities are routinely cited in vulnerability assessments, often including warnings of unapplied security patches and existing Technologically Feasibility Exceptions (TFE).

vi. Infiltration of "Internet of Things" (IoT)

Before the IoT became common, mundane equipment such as uninterrupted power supplies (UPS), heating ventilation and air conditioning (HVAC), closed circuit television cameras (CCTV), and other devices common in regulating the physical data center environment were not a security concern as they were typically not network-capable. Now, manufacturers are incorporating network connectivity in almost all appliances, including refrigerators, toasters, ovens, microwaves, and coffee makers. Not surprisingly, these appliances, once introduced into even non-secure areas such as a control center breakroom, could pose a threat to the utility network. Therefore, continuous passive monitoring for unknown devices on ESP networks may help to identify their presence.

F. Non-Technical Cyber Security Issues Facing the Grid

i. Vendor Responsibility and Accountability

The role and importance of a SCADA vendor cannot be overstated. The level of service and responsiveness of technical support from the vendor should be considered with just as much weight as the capabilities of the architecture itself. Along with support considerations, vendors should also be examined for how robust and effective their internal controls are, and how they handle customer data, specifically NERC CIP protected information about BES Cyber Assets.

Vendors are not independently accountable to NERC, but are required to comply with NERC CIP. This includes conducting background checks and controlling access to any NERC CIP sensitive information they may have.

While vendors can provide expertise on the SCADA systems, they are not necessarily experts on NERC CIP requirements. Furthermore, each customer can have very different positions regarding some of the more ambiguous requirements. As a result, NERC CIP compliance is a very difficult issue and is often a moving target for what is required for one customer (based on policy), and what is required for another. It is therefore up to the responsible entity to ensure that vendors, who commonly hold the keys to their crown jewels, are taking that responsibility seriously by using strong internal controls, even when they're not actively connected inside the responsible entity's Electronic Security Perimeter (ESP).

An example of this scenario occurred in 2015, when a vendor went on-site to a customer to apply updates to a SCADA database.[47] Her escort discovered that she had all the customer's system accounts and passwords written down in a ragged spiral-bound notebook she had carried with her.[48] Upon further inspection, the customer

47 The above scenario transpired while the co-author, Joel Gridley, was performing a site-visit at an unnamed client.

48 *Id.*

also discovered that other sensitive information, such as host names paired with IP addresses and operating systems, was also in the notebook.[49] These notes were likely kept with the goal to improve the vendor's customer support (and for the sake of convenience), but this was a possible violation that needed to be self-reported to the Regional Enforcement Entity. Regular dialogue between the vendor and the customer, along with a review of internal control assessments, could have prevented the possible violation.

Language should be considered in service contracts to address the risks that vendors represent. There is a lot of trust placed in them to handle sensitive information, and there is an expectation to protect that data with appropriate technical and procedural controls—with built-in oversight and perhaps even possible sanctions by the customer.

ii. Legacy "If It's Not Broken, Don't Fix it" Mentality

The utility industry's unspoken *de facto* position has historically been, "if something isn't broken, don't meddle with it" for the fundamental reason that functioning mechanical equipment had no need to be disturbed, and if it were disturbed, it would often result in unintended consequences. Today, the technologically sophisticated Smart Grid requires nearly constant maintenance to ensure reliable operation. Regular updates and emergency security patches are a common occurrence. Far too many dispatchers and operators cringe at the thought of tinkering with a grid that appears to be humming along. While historically a sound strategy, failing or refusing to update the modern Smart Grid ensures that it will quickly become outdated or vulnerable to malicious or inadvertent disruption.

49 *Id.*

iii. Positions Based on Ease of Meeting Compliance

Throughout the NERC CIP standards there are requirements with language that reads, "Identifies, assesses, and corrects . . ." (IAC).[50] Many of these IAC requirements include general guidance on topics the policy or process is required to address, but give room for the responsible entity to include more refined details surrounding those processes. For example, CIP-006R2.1 requires an IAC documented visitor control program to "*Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances.*"[51] This may provide the utility with a basic framework to develop a program, but it lacks specificity regarding how many visitors a single escort can bring into the environment per trip or while logged in (as required by CIP-006R2.2), for example, or whether the escort is required to accompany the visitor during brief trips outside the physical security perimeter (such as bathroom breaks). Many NERC CIP standards leave these additional details up to the individual responsible entity. As a result, utilities may be unknowingly creating a standard that they are held to in the future by the NERC regulators.

There are two scenarios in which responsible entities can get into trouble. One causes compliance issues, and the other causes security issues. The first occurs when well-intentioned managers create utopian policies: requirements that are extremely conservative and demanding, but completely infeasible to follow for lack of staff, technology, or process. Often, such policies result in the utility answering uncomfortable questions from regulators.

---

50 *Transition Program FAQs*, North American Electric Reliabilty Corp., http://www.nerc.com/pa/CI/Pages/Transition-Program-FAQs.aspx (last visited Feb. 8, 2017) [hereinafter Transition Program].

51 *CIP-006-6 Cyber Security: Physcial Security of BES Cyber Systems*, North American Electric Reliability Corp., http://www.nerc.com%2Fpa%2FStand%2FPrjct2014XXCrtclInfraPrtctnVr5Rvns%2FCIP-006-6_CLEAN_06022014.pdf (last visited Feb. 8, 2017).

The second instance is not so easy to discover, as the policies developed will satisfy the letter of the requirements, but fall shy of following security best practices. Merely having check boxes for the existence of the policy and evidence the policy is followed may result in the appropriateness of the policy itself being overlooked.

Similarly, ambiguous terminology such as *custom software* from CIP-010R1.1 which requires a corporate legal position, or doctrine as to how the responsible entity defines the ambiguous term (and therefore audited against the position) can also fall into the two traps mentioned above.[52] In the example given, a comprehensive and all-encompassing definition will quickly become onerous and cumbersome for compliance purposes, but a definition with strict limitations on what is included can expose the environment to risk.

Introduced in NERC CIP v5 is the concept of "Transient Devices" and allowance of "Removable Media" in CIP-010R4.[53] These can be easily abused for the sake of convenience while complying with the letter of the requirement, but careful consideration must be made to ensure that security best practices are maintained.

iv. Compliance Staff Lacking Technical Skills

Compliance staff oversee and manage all aspects of compliance, including supervising and managing the gathering of evidence, composing Reliability Standard Audit Worksheets (RSAWs), and submitting TFEs and self-reports. However, they do not always have a technical background and often rely heavily upon the IT Operations staff for terminology, evidence gathering, and mitigation suggestions. Much of the information collected from the IT Operations staff must be taken at face value, since the

52 *CIP-010 Cyber Security: Configuration Change Management and Vulnerability Assessments*, North American Electric Reliability Corp., http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-010-2&title=Cyber%20Security%20-%20Configuration%20Change%20Management%20and%20Vulnerability %20Assessments (last visited Feb. 8, 2017) [hereinafter Configuration].

53 *Id.*

compliance staff may not have the technological expertise to challenge or question the information.

Because of the additional expense of clearing other corporate resources with technical expertise who would be able to review the provided information with objectivity, this option is often not leveraged. An objective eye with technical expertise is required to preserve true separation of duties. Therefore, there is yet another opportunity for things to be missed either intentionally or unintentionally with no system of checks and balances in place.

v. Critical Infrastructure Regulations

Pursuant to the Energy Policy Act of 2005, the power industry is regulated by mandatory cyber security standards.[54] These regulations fall within the jurisdiction of the Federal Energy Regulatory Commission ("FERC").[55] The cyber security standards are developed by the North American Electric Reliability Corporation ("NERC").[56] NERC is a not-for-profit international regulatory authority that covers the continental United States, Canada, and the northern portion of Baja California, Mexico.[57] NERC relies on industry experts and government representatives at both the state and federal level to formulate its cyber security guidelines.[58] Once developed, they must be authorized by Congress, then reviewed and approved by FERC.[59] The reliability standards that govern the three interconnected power grid systems were developed by the electric power industry, and then approved by FERC to ensure interoperability and coordinated

54 Energy Policy Act of 2005, Pub. L. No. 109-58.

55 *Frequently Asked Questions About Cybersecurity and the Electric Power Industry*, Edison Electric Inst., http://www.eei.org/issuesandpolicy/cybersecurity/documents/cybersecurity_faq.pdf (last visited Nov. 23, 2016) [hereinafter EEI].

56 Transition Program, *supra* note 49.

57 EEI, *supra* note 54.

58 *Id.*

59 *Id.*

electrical systems.[60]

NERC standards are only applied to utilities that fall within the definition of Bulk Electric System (BES).[61] Currently, the definition for BES includes all transmission elements operated at 100 kilovolts (kV) or higher, as well as real or reactive power connected at 100kV or higher.[62] NERC CIP 002-5.1, however, defines a BES as including Distribution Providers that own facilities, systems, and equipment that is: (1) an under frequency load shedding (UFLS), or (2) an under voltage load shedding (UVLS) program that is subject to NERC/Regional Reliability Standards, or (3) performs automatic load shedding under a common control system of 300MW or more (without human intervention).[63]

This raises an issue, as NERC's CIP regulations and FERC's reliability mandates will not apply to facilities below these thresholds. Thus, attackers could potentially use these non-covered entities as backdoor access points for cyber intrusions.[64] Additionally, BES systems are further classified as either high impact or medium impact.[65]

For BES, FERC has approved eleven critical infrastructure protection CIP stan-

60 *Id.*

61 *Id.*

62 FERC Order No. 693, FERC Stats. & Regs. 31,242 Mandatory Reliability Standards for the Bulk-Power, 693 Fed. Energy Reg. Comm. ORD. § 4.2 (Mar. 17, 2007).

63 *CIP-002-5.1 Cyber Security: BES Cyber System Categorization*, North American Electric Reliability Corp., http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-002-5.1&title=Cyber%20Security %20%E2%80%94%20BES%20Cyber%20System%20 Categorization&jurisdiction=null (last visited Dec. 29, 2016) [hereinafter BES Cyber].

64 Consider, for instance, data breaches such as the Target data breach wherein 45 million card numbers were exfiltrated by attacking Target's databases through an unsecured backchannel built to allow their HVAC supplier to remotely access monitor and control on-site systems. Here too, in an interconnected framework it is feasible that an attacker could target (no pun intended) smaller, non-BES entities that are not NERC CIP compliant and use that to elevate privileges and access BES entities. Meagan Clark, *Timeline of Target's Data Breach and Aftermath: How Cybertheft Snowballed for the Giant Retailer,* Int'l Bus. Times (May 5, 2014), http://www.ibtimes.com/ timeline-targets-data-breach-aftermath-how-cybertheft-snowballed-giant-retailer-1580056.

65 BES Cyber, *supra* note 62 (High Impact and Medium Impact are defined in CIP 002-5.1).

dards, which are focused specifically on cyber security. Additionally, in February 2013, President Obama issued executive order (EO) 13636: Improving Critical Infrastructure Cyber Security, along with a Presidential Policy Directive (PPD) 21. Specifically, EO 13636 calls for the following[66]:

- Developing a technology-agnostic cyber security framework;
- Promoting and incentivizing the adoption of cyber security practices;
- Increasing cyber threat information sharing;
- Leveraging privacy and civil liberties protections within any initiative to secure critical infrastructure; and
- Exploring the use of pre-existing regulations to promote cyber security. Whereas, PPD-21 advocates for:[67]
- Developing situational awareness to address physical and cyber elements of infrastructure in real-time;
- Analyzing and understanding the potential cascading consequences that might arise from infrastructure failures;
- Evaluating and improving the partnership between the private and public sector;
- Evaluating and updating the National Infrastructure Protection Plan; and
- Developing a comprehensive research and development plan.

The current NERC CIP regulations include the following:[68]

- CIP 002-5.1: Cyber Security - BES Cyber Systems
- CIP 003-6: Cyber Security - Security Management Controls Categorization
- CIP 004-6: Cyber Security - Personnel & Training
- CIP 005-5: Cyber Security - Electronic Security Perimeter(s)
- CIP 006-6: Cyber Security - Physical Security of BES Cyber Systems
- CIP 007-6: Cyber Security - Security System Management
- CIP 008-5: Cyber Security - Incident Reporting and Response Planning
- CIP 009-6: Cyber Security - Recovery Plans for BES Cyber Systems

---

66 *EO 13636 and PPD-21*, Dep't Homeland Sec., https://www.dhs.gov/sites/default/files/publications/EO-13636-PPD-21-Fact-Sheet-508.pdf (last visited Nov. 23, 2016).

67 *Id.*

68 *CIP Standards: Subject to Enforcement*, North American Electric Reliability Corp., http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx (last visited Dec. 15, 2016).

- CIP 010-2: Cyber Security - Configuration Change Management and Vulnerability Assessments
- CIP 011-2: Cyber Security - Information Protection Standard
- CIP 014-2 Physical Security69

For this white paper, we focus on the following NERC CIP guidelines:

CIP 005: The establishment of electronic security perimeter conclaves within a corporate environment are exceedingly difficult to implement and maintain under ideal conditions. This should, however, be taken in the context of the President's Cybersecurity Commission report released in November 2016, which stated that enterprise electronic security perimeters are outdated, outmoded, and ineffective. This is an interesting regulation which is increasingly dynamic.

CIP 007: This regulation includes the bulk of the operational implications of daily cyber security tactics that an entity will need to perform. A lot of "the what," "the when," and "the where," is described and this information is critical for IT operations.

CIP 008: From an operational perspective, this piece is critical. From a liability and legal exposure perspective, the creation, adoption of, and adherence to this CIP is essential. While this is a proactive regulation implemented to manage a post-incident reactionary response, here the focus is going to be on the legal side.

CIP 009: This is the IT operational analogue to the legal issues and reporting requirements under CIP 008. This would generally be an aspect or even the driving force behind a comprehensive disaster recovery plan. As with any DR plan, creation and implementation are largely prophylactic unless applied within actual testing scenarios.

CIP 010: Within this regulation, the potential for ongoing and daily impacts to IT operations is significant. The policies and procedures must be developed and fully implemented across the organization. While the human element is often regarded as

69 While NERC lists this as "subject to enforcement" this CIP has not yet been adopted and is pending. *Id.*

the weakest link, the use of systems and software that are not patched to address known vulnerabilities is certainly near the top of that same list.

Because of the CIP cyber security standards and those dictated by EO 13636 and PPD-21, the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) was created and has been used to share threat information between the public industry and private sector entities.[70]

vi. Critical Infrastructure: Legal Implications

Depending on "the how, and the where" from which an attack is initiated, and depending on who the attacker is, there are varying cyber security implications.[71] Likewise, in the realm of the power grid, the legal implications are quite different from those which a typical company or industry may encounter. In the power industry, while PII certainly exists and is collected and stored, the richer targets are the operations themselves and the continuous flow of electricity. Thus, it is less likely that a BES will need to focus on data breaches and breach notification laws; and instead will need to focus on the legal implications they may face in the case of a cyber-event that results in loss of power.[72] Furthermore, in this industry, it is far more likely that a cyber-event could have material impacts on quality of life. There is a potential for loss-of-life circumstances that would be the natural result of a sustained power loss situation in either extreme hot or cold weather conditions.

Additionally, the mere fact that the power grid is included within critical infrastructure underscores the national security implications inherent in continuous and reliable power transmission. Therefore, this industry differs significantly from the retail

---

70 Joseph S. Abrenio, *Illuminating Issues of Grid Cybersecurity*, U.S. Cybersecurity Mag., http://www.uscybersecurity.net/united-states-cybersecurity-magazine/fall-2016/mobile/index.html#p=Cover (last visited Feb. 7, 2017).

71 Roland L. Trope & Stephen J. Humes, *Before Rolling Blackouts Begin: Briefing Boards on Cyber Attack that Target and Degrade the Grid*, 40 Wm. Mitchell L. Rev. 647 (2014).

72 *Id.* at 756-57.

or entertainment industries where a cyber-event could be a nuisance, and could affect large numbers of individuals in a financial sense, but is unlikely to have even a tangential relation to national security.

Consequently, it is increasingly likely that a targeted attack against the grid would result in ongoing and after-action coordination with state and federal authorities versus a purely private sector response. Considering the greater potential for a national response to a grid cyber-event, the onus is even higher for a complete and thorough analysis of the operations to provide a high level of confidence as to the timing of any breach, and as much metadata as possible to ensure accurate event tracing.

vii. Risk Mitigation

To mitigate risk, many areas can and should be addressed. A prominent area of focus needs to be compliance with NERC CIP policies. Grid utilities that operate below the designated BES thresholds should consider adopting all or at least portions of the NERC CIP regulations to demonstrate compliance and reduce overall liability. Obviously, any utility designated with BES status should and must comply with both the spirit and the letter of the NERC CIP policies. Consequently, if risk mitigation is a primary motivator, then any BES should strongly consider conducting a third-party vendor assessment of any non-BES utility that has interconnections with the power grid. This is merely one piece in a much larger mosaic that paints a picture of cyber security.

G. Best Practices

Whereas the regulatory framework provided by NERC/FERC provides basic guidance, the framework should be viewed merely as the minimum baseline and aspirational in nature. Given the ever-changing technology landscape, cyber threats are dynamic. Entities must meet the baseline defenses while moving towards higher levels of cyber security to forestall any issues. Resilience and security are long-term goals which do not comport themselves to rigid, static guidelines. Rather, the operators in this space

must remain vigilant to develop, maintain, continuously expand, and adapt their cyber security practices.[73]

H. Human Assets and Resources

System Operators and Dispatchers are those professionals tasked with management, operation, and reliability of the BES.[74] System Operators and Dispatchers are certified and credentialed through NERC, which maintains those credentials and modifies training and testing requirements as needed.[75] After becoming certified as a System Operator or Dispatcher, the credential must be maintained through continuous education and training.[76] Additionally, each Regional Transmission Organization (RTO) requires certification of Operators and Dispatchers for both Transmission facilities and Generation facilities.[77] Because of this disciplined approach, Operators and Dispatchers are equipped with the basic knowledge required to perform their roles.

IT System Administrators are professionals within the computing industry responsible for maintenance and administration of cyber assets, which support the BES. In contrast to the credential requirements of the Operations staff, the IT Operations staff have no NERC or RTO sponsored certifications.[78] Even those requirements articulated in CIP-004 have no formal curriculum allowing regulated utilities to develop their own individual training which can take the form of anything from an email, reading course handouts, live classes, or navigating through a multi-media online seminar.[79] Testing of

---

73 Abrenio, *supra* note 69.

74 *System Operator Certification*, North American Reliability Corp., http://www.nerc.com/ pa/Train/SysOpCert/Pages/default.aspx (last visited Feb 8, 2017).

75 *Id.*

76 *Id.*

77 *Id.*

78 *CIP-004-6 Cyber Security: Personnel & Training*, North American Reliabilty Corp., http://www.nerc. com/pa/Stand/Prjct2014XXCrtclInfraPrtctnVr5Rvns/CIP-004-6_CLEAN_06022014.pdf, (last visited Feb. 8, 2017).

79 *Id.*

the curriculum is also optional.[80]

There are computer and security industry certifications such as the CISSP and GIAC, which regulated entities can require of their IT System Administrators but are not required by NERC.[81] It seems to be an oversight to require NERC and RTO regulated credentials for the System Operators and Dispatchers to protect critical assets, but to have no such requirements for the IT System Administrators who have system-level access to critical cyber assets which support, manage, or monitor those same critical assets.

While System Operators and Dispatchers have expertise in BES, and IT System Administrators have expertise in computers, applications, and routing protocols, the esoteric nature of individual SCADA systems leave both groups sometimes wholly dependent upon the SCADA vendor for expertise. In daily operations, this is not an issue, since most SCADA vendors provide excellent support and responsive service. However, vendors are not always included in all projects within the ESP. This exclusion can sometimes lead to unintended disruption.

Vendors have become a popular attack vector for intrusions in many industries, and SCADA vendors—given their requirement for remote access into systems within the ESP to provide support—are an attractive target of malicious actors. Unfortunately, the security practices claimed by a SCADA vendor are typically not verified by their utility customers beyond what they need to satisfy CIP-004 for personnel risk assessments. While NERC CIP is indeed on the forefront of compliance requirements which make sense, it falls far short of the Federal Financial Institutions Examination Council's (FFIEC) requirements for examinations of Technology Service Providers (TSP). Because NERC does not require it, it is left up to each regulated entity to decide how much due diligence it will perform, and at what intervals to ensure they are not put at risk by

80 *Id.*

81 *Id.*

allowing remote interactive access into the ESP by the SCADA vendor.

I. Conducting Assessments

Vulnerability Assessments (VAs) required by NERC CIP-010 R3.1 is not necessarily the security industry's definition of a vulnerability assessment. "Active" VAs in CIP-010 R3.2 and R3.3 adhere more to the security industry definition. Per Reliability First, a Regional Entity with delegated enforcement authority from NERC, the minimum requirements for a vulnerability assessment are:

- Network and access point discovery;
- Port and service identification;
- Review of default accounts, passwords, and network management community strings; and
- Wireless access point review.[82]In the "Guidelines and Technical Basis" section of CIP-010 for Requirement R3, these minimum requirements are further explained:[83]

Paper Vulnerability Assessment:

1. Network Discovery - A review of network connectivity to identify all Electronic Access Points to the Electronic Security Perimeter.
2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification.
3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings.
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications.

Active Vulnerability Assessment:

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification - Use of active discovery tools

82 Rhonda Bramer, Frank Kapuscinski, & Scott Pelfrey, *CIP-010 CIP V5 Worksho*p, Reliability First, https://rfirst.org/compliance/Documents/RF%20CIPv5%20Workshop%20CIP-010.pdf (last visited Dec. 27, 2016).

83 Configuration, *supra* note 51.

(such as Nmap) to discover open ports and services.

3. Vulnerability Scanning - Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning - Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within range of the wireless scanning tool.

One should note, there are no mention of authentication certificates, public/private keys, or shared secret keys. As best practice, consider taking inventory of these authentication types in use, and incorporate them into your password management program and processes. To prevent Protected Cyber Assets ("PCAs") from becoming Electronic Access Control or Monitoring Systems ("EACMS"), limit use of authentication certificates from PCAs to other BES cyber assets, as this would indicate the PCA controls access to the remote BES cyber asset it is connecting to, and could arguably be considered an EACMS with all the accompanying requirements.

Another best practice is during the vulnerability scanning, and network port and service identification phases of active vulnerability assessments, to confirm validity of the information documented for each cyber asset for CIP-007R2.3 and CIP-010R1.1. Much of this information can be used as evidence to satisfy related requirements. Unless the BES Cyber Assets are highly unstable, it is recommended to perform the active vulnerability assessments whenever possible. The process is generally more streamlined, with standard output, and as seen above, much more comprehensive to support a secure computing environment.

i. Addressing Legal Liability

Given the fact that the application of cyber security standards to the grid is a relatively new development, there is little case law directly on point that deals with utility company liability in cases where the NERC CIP standards were not fully adhered to when a breach or outage occurred. The Federal District Court in *Waldon v.*

Ariz. Pub. Svc. Co. held that non-utility customers lacked standing to initiate a case, and specifically held that while NERC standards created a duty between the government and utility suppliers, no similar duty was created with utility customers.[84] According to the American Public Power Association (APPA), negligence claims arising from a failure to prevent against cyber-attacks could expose electric utilities to liability.[85] Furthermore, APPA asserts that while states have considered legislation that would limit utilities' liability for cyber-attacks, there are currently no federal or state statutes in place that provide immunity from liability merely for adhering to cyber security standards.[86]

However, there are several cases in which enforcement actions were taken, penalties were assessed, and remediation procedures and processes were recommended. Of course, by their very nature, these violations occur within critical infrastructure. Consequently, some portions or identifying characteristics are removed from the public versions of these orders and stipulations.

For instance, in one case where an entity had failed to comply with portions of CIP-002-3, CIP-005-3s, CIP-006-3c, and CIP-007-3a the Unidentified Registered Entity (URE) was assessed a penalty of $250,000.[87] In another case, a URE was determined to have violated 19 CIP standards, with the root cause being the URE's failure to create and utilize a comprehensive change management plan which resulted in a lack of independent inspections of new substations to identify Critical Cyber Assets (CCAs),

---

84 642 F. App'x 667, 669 (9th Cir. 2016).

85 *In Support of Appropriate Liability Protection for Electric Utilities Related to Cyber Attacks*, Am. Pub. Power Ass'n (June 17, 2014), https://www.publicpower.org/files/PDFs/Resolution%20 14-08%20--%20Liability%20Protection%20for%20Utilities%20Related%20to%20Cyber%20 Attacks%20--%20FINAL.pdf.

86 *Id.*

87 *NERC Full Notice of Penalty regarding Unidentified Registered Entity*, North American Electric Reliability Corp. (Oct. 31, 2016), http://www.nerc.com/pa/comp/CE/Enforcement%20 Actions% 20DL/Public_FinalFiled _NOP_NOC-2492.pdf (In this case, all of these violations were noted during a self-reporting and self-certification process which the URE undertook. In each case the potential risk was deemed as moderate.).

EACMs, and Physical Access Control Systems (PACS).[88] In this case, the URE was assessed a penalty of $1,125,000 as the nature of the risk was deemed to be serious.[89]

While there are potential FERC penalties that may be enforced with respect to liability due to outages, it is difficult to litigate against a utility, as a claimant would have to establish a basis for negligence. When dealing with risk of harm or loss of life, the calculus results in a lower burden for the claimant (essentially when the claim involves risk of harm or actual harm/death the claimant's case is more straightforward, and more likely to survive a dismissal motion in a pre-discovery context). For a cause of action to survive a motion for dismissal, the plaintiff must demonstrate standing to sue which requires actual injury.[90]

Therefore, even though it would be a difficult task for an end-user, consumer, or business customer of a utility to demonstrate standing, there are multiple instances of penalties, fines, and process modifications imposed by FERC on entities that violate the NERC CIP policies. Even where the names and details remain confidential, the impact on the entity through ongoing monitoring and compliance checks in addition to any financial penalties should give pause to investors considering their options within this industry. Furthermore, were an entity to be sanctioned by FERC, that sanction could also be used against them should a case or controversy arise and should standing be properly asserted.

There are two basic tests to prove standing, the first is a Constitutional test which requires the following: (1) the plaintiff must allege that they have suffered or

---

88 *NERC Full Notice of Penalty regarding Unidentified Registered Entity*, North American Electric Reliability Corp. (Oct. 31, 2016), http://www.nerc.com/pa/comp/CE/Enforcement%20Actions% 20DL/Public_FinalFiled_NOP_NOC-2450.pdf.

89 *Id.* (Note: while the opinion referenced CCAs, in CIP V5 this terminology was updated to reflect BES Cyber Asset. The use of the term CCA was included merely because that was the exact verbiage utilized within the FERC opinion.).

90 *Supra* note 83.

imminently will suffer an injury; (2) the plaintiff must allege that the injury is fairly traceable to the defendant's conduct; (3) the plaintiff must allege that a favorable decision by the court would redress the injury.[91] The second basic test is referred to as the "prudential" test and states: (1) a party may only assert their own rights and not the rights of others; (2) a plaintiff may not sue merely as a class of taxpayers asserting the rights of the entire class; (3) a claim may only be raised if it is within the zone of interests protected by the statute in question.[92] Finally, it is possible to assert associational standing, whereby an association may show standing to sue on behalf of its members.[93] This too, imposes a three-part test: (1) the members must otherwise have standing to use on their own; (2) the interests being sought are germane to the organization's purpose; and (3) neither the claim asserted nor the relief requested requires the participation in the lawsuit of the individual members.[94]

It is easy to see how difficult it would be to sue an entity for a power outage or a voltage line fluctuation that arose as the result of a cyber-incident. Therefore, it is far more likely that an entity would face sanctions from the FERC than redress from a court of law. However, under NERC CIP 008, the responsible entity must develop and maintain a cyber security incident response plan and must have processes and procedures in place to identify, classify, and respond to cyber security incidents.[95] Within the classification, a responsible entity must determine whether an event is either reportable or non-reportable. In the case of reportable events, the ES-ISAC must be notified within

---

91 Ne. Fla. Contractors v. Jacksonville, 508 U.S. 656, 663-64 (1993).

92 Lujan v. Defs. of Wildlife, 504 U.S. 555, 576-78 (1992).

93 Hunt v. Wash. State Apple Advert. Comm'n, 432 U.S. 333, 343 (1977).

94 *Id.*

95 *CIP-008-5 Cyber Security: Incident Reporting and Response Planning*, North American Electric Reliability Corp. (July 9, 2014), http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-008-5&title=Cyber%20Security%20-%20Incident%20Reporting%20and%20Response%20Planning&jurisdiction=null.

one hour of the cyber event.[96]

ii. Risk Transference

It has often been said that no one wants to pay for insurance when things are going well but as soon as things go awry everyone wishes they had insurance. The world of cyber security is no different with major data breaches hitting the headlines. The costs of downtime to utilities both in a purely economic sense in addition to the potential for loss of life, is a very real concern. While we would argue that cyber security insurance is a "should have" for any utility, for the BST entities with no other option, cyber security insurance is a "must-have."

In addition to understanding cyber security issues and taking steps to address them, utilities should prepare for a cyber security incident by procuring insurance policies to attain coverage for anticipated events. Utilities need to take a best practices approach when evaluating a cyber security policy and managing compliance overall.

With respect to insurance policies, it is important to note the two main types of policies: (1) first-party policies—which cover losses directly incurred by the policy-holder and (2) third-party policies—which cover a policyholder's liability to third-parties.[97] Under the first-party policy, a grid utility could have coverage that would include unplanned shutdowns or outages as such might occur in a cyber-attack.[98] Typically the deductibles for such a policy would be expressed in terms of time (e.g. insurer pays in excess of D days; or H hours, etc.). However, most insurance policies require physical damage so in the case of a cyber-attack that causes operational issues with the Smart Grid, it may prove difficult to establish that actual physical damage occurred and thus

96 *Id.* (One hour refers to a preliminary notification which is often informal (online, via phone) and submitted within one hour of determining that a reportable cyber event occurred.).

97 Erin L. Webb, *The Internet of Things: Cybersecurity, Insurance, and the National Power Grid*, 30 Nat. Resources & Env't 35 (2016).

98 *Id.*

the insurer may not be required to compensate. Thus, policyholders must carefully review their policies to ensure that software and device issues are not excluded. Otherwise a pure cyber-attack with no kinetic component could result in huge losses to a utility which would not be covered under their insurance policy. The same could happen with respect to third-party coverage. Given the fact that an attack on the grid could potentially result in physical damage to persons, grid entities must review their policies to verify that they have either general commercial or cyber coverage that includes both physical and non-physical losses.[99] Otherwise, they could expose themselves to significant risk if they fail to account for both potential types of loss.

Conclusion

We live in a connected world where critical infrastructure in general and the power grid specifically play vital roles. Without a consistent and reliable supply of electrical power throughout North America, nearly every aspect of everyday life would be negatively impacted. In the event of a long-term outage (more than a couple of days) that covers a wide area, the economic impacts would be staggering. Were such an outage to occur during either cold or heat temperature extremes, the loss of life could number in the tens or hundreds of thousands. These are very real and very dire implications that will arise should the power grid suffer an outage.

This paper discussed some of the implications of a power outage and looked directly at the cyber security implications for the grid utilities. Furthermore, it outlined how utilities can bolster their cyber security and mitigate some of the risks that they face. No one would deny the importance of the power grid within a critical infrastructure paradigm. Following the widespread media coverage of high profile cyber-incidents (the Sony Hack, the Stuxnet Virus, the OPM data breach) no one is denying the fact that cyber-attacks are occurring all around us. Consequently, security through obscurity

99 *Id.*

is a fools' errand. Grid utility companies must face the reality within which they now operate; cyber-attacks are ongoing, and any industry within the critical infrastructure framework is going to be an attractive target for a myriad of reasons.

As we outlined, following the NERC CIP guidelines is a very good first step towards addressing cyber security needs and issues. However, that in and of itself is not enough. Grid utility companies must embrace the stark new reality and consider the implications of everything they do within all the areas in which they operate. The costs of baking-in cyber security in a technical sense to their ICS and SCADA systems must be balanced against the potential costs that a widespread outage could inflict both financial loss as and legal liability.

Grid utility companies must move towards greater cyber security hygiene. This includes both technical and non-technical issues facing the grid as well as the human element which is often the weakest-link in any cybersecurity initiative. The cost of doing nothing is too great. In an uncertain legal world, mere compliance with NERC CIP guidelines may also be insufficient to avoid legal liability. Therefore, companies should take a proactive approach to ensure that cyber security is not an afterthought or a check-mark on a framework. Cyber security must be an integral part of each and every project, and considered within every aspect of the grid utility operations.

Future Crimes

Reviewed by Jeffrey Cullen

Citation: Marc Goodman, *Future Crimes* (Doubleday, 2015).

Relevant Legal and Academic Areas: Criminal Law, Constitutional Law, Privacy Law, Information Technology, First Amendment, Fourth Amendment, Social Media

Summary: *Future Crimes* is a wakeup call to the threat of newly emerging technologies and the threat that they pose to everybody's security. Goodman explains that our society is on the brink of further advancements in technology that will connect society to the Internet is many aspects. Goodman explains just how insecure our information on the Internet is and the dangers that are accompanied with this vulnerability. Goodman identifies that we are all at risk of misappropriation of our information and society must be proactive to take back the control of the devices that we have created.

About the Author: Marc Goodman is a global strategist and author whose focus is on next generation security threats such as cyber crime and cyber terrorism. Goodman has worked extensively as a Senior Advisor with INTERPOL to train the police forces of many nations about the next generation security threats. Goodman is also the founder of the Future Crimes Institute to educate others on the security and risk implications of newly emerging technologies. Goodman seeks to raise awareness about the threat of emerging technologies and the risks that they pose to the security of the general public.

Introduction

We live in a civilization that is deeply interconnected yet technologically insecure. People use a variety of technologies and services that are connected to the Internet. Our world has evolved into societies that depend on technology on a daily basis. Although these new technologies are innovative, convenient, and beneficial, there is a significant amount of information unknown to the vast majority of users. The data that

(and many other technological devices) we create information that is collected and stored by a variety of entities. Our use of the Internet shows these entities an infinite list our most intimate and individual characteristics including our finances, family, relationships, search history, and behavior. *Future Crimes* is a wakeup call to the threat of these newly emerging technologies and the threat that they pose to everybody's security.

The information we create about ourselves is not secure and is susceptible to being sold by data brokers, or worse, stolen by criminals. Today, "[w]e are being penetrated, digitally probed, spied upon, robbed, and virtually manipulated day in and day out, and most of us remain blissfully unaware of the threat. Welcome to the new normal, a world in which for every screen in your life governments, criminals, terrorists, and hactivists have a plan of attack." *Future Crimes* opens readers' eyes to the imminent threat we all face in today's technological world. Goodman emphasizes, "[b]efore we add billions of hackable things and communicate with hackable data transmission protocols, important questions must be asked about the concomitant risks with regard to the exponential implications for the future of security, crime, terrorism, warfare, and privacy."

Evolution of Crime

"[I]n order for us to understand the vast technological threats before us, we must understand our enemies." Prior to our technological advancements, if a criminal were was looking to acquire money, he would have to physically park a car, enter a bank, pile money into a bag, and make a getaway. Today, with the evolution of technology, that type of crime is insignificant. Organized crime groups have now diverted their resources from physical criminal activities to "take advantage of the easy profits, greater anonymity, and limited police scrutiny afforded in cyberspace." Today, there are many parties that use the Internet against its users, including nation governments, hacktivists, military personnel, and transnational organized crime groups. Organized crime groups have moved from their physical crimes to more detrimental crimes including identity theft, credit

card fraud, and tax fraud. The limited amount of security is due in part to the nature of the Internet. People are now capable of extending their reach across the world without ever leaving their country, much less their chair. Unlike in the physical world, there are no borders defining where one nation's jurisdiction begins and where another nation's jurisdiction ends.

Criminal Minds

The threat of security breaches prompts consumers and businesses to invest millions, cumulatively billions, of dollars every year to protect their information from malware, which is software that is intended to damage an individual's computer system. Unfortunately, the reality is that the programs we invest in to protect us only catch about five percent of the threats to our systems. Goodman analogizes to this statistic: "[i]f your body's own immune system had a batting average like that, you would be dead in a matter of hours." This threat to our systems is proliferated by criminals' and virus writers' ability to out-innovate and out-maneuver the antivirus industry created to protect us. Further statistics show that in sixty-two percent of instances where hackers infiltrate a business, it takes at least two months before the intrusion is even detected. This disturbing information means that a hacker has the time to sit and watch your system, your virtual activities, gather information about your finances, personal characteristics, and contacts, for a long period of time before being discovered. By that time we have likely already lost the battle and the hacker has succeeded in gathering our information and can use it however he wants.

The ease with which criminals can access our supposedly private computers and networks is disturbing. "According to the Verizon study, once hackers set their sights on your network, 75 percent of the time they can successfully penetrate your defenses within minutes." This means that we are all sitting ducks. It is only a matter of time until a hacker comes around to target you and when he does, you are at the hacker's

mercy. People are hacked and suffer from crimes such as identity theft on a daily basis yet somehow, we think we are immune. We do not feel threatened by hacking simply because these crimes occur in a virtual realm where our understanding is scant. However, that is all the more reason to be concerned. We are inputting our most intimate and most important information onto the Internet, into a "cloud" that we understand very little about. How does it function? Where is our information being stored? Who has access to our information? How secure are these virtual vaults that store our information? Internet crimes are the future of criminal activity and are ever more threatening than any physical crime within the same sphere. We must identify and find a way to eliminate these risks because nobody is safe.

Phishing is a pervasive risk to anybody who uses technology. Phishing is the technique hackers use to get innocent people (fish) to take the bait of a malicious link that is disguised as being a genuine site. The purpose of hackers' phishing is to trick unsuspecting users into clicking on links that take them to fake websites or install malware on their device. "Phishing messages arrive in our in-boxes, via SMS, tweets, instant messages, and Facebook status updates. They allegedly come from our banks, cable companies, retirement plans, social media outlets, and mobile phone operators and target users around the world..." A false message appears in every way to resemble a real message from the true sender because of the nature of the Internet. If somebody types "*security@bankofamerica.com*," that is how it will appear to the person receiving the message. Usually phishing messages prompt you to click a button by notifying you that your password or other information needs to be updated. Once you click that button, the hackers will have access to all of your personal and financial information. Phishing is considered to be a gateway crime "that provides thieves with the data they need to perpetrate... identity theft, financial fraud, tax fraud, and insurance fraud." Once a hacker has successfully phished your information, they can wreak havoc.

Coca-Cola, along with many large corporations, have fallen victim to phishing. In one instance, Coca-Cola's deputy president opened an email that was spoofed to appear as if it came from a senior executive and contained a relevant subject line. "The perpetrators of the attack spoofed reality by making the message appear as if it came from a trusted colleague, on the internal corporate network, with a subject line that was compelling and contextually made sense." When the deputy president clicked on the link, malware was downloaded onto Coca-Cola's system. The hackers were then able to see in real time what was being typed on Coca-Cola's computers and were able to download many computer files related to a major deal. As a result of this one phishing attack, Coca-Cola lost $2.4 billion that it would have obtained from the deal.

Hackers can also impersonate other people and entities. Goodman discussed the hacker Mark Jakob, who created a fake press release and about the Emulex Corporation, a Nasdaq-traded communications equipment manufacturer. "The hacker merely copied the stationery and style of previous Emulex press releases, spoofed the company's e-mail address, and forwarded his news story to the Internet Wire. The fictional press release stated the SEC had opened an investigation into Emulex, that its quarterly earnings were to be restated, and that the company's CEO, Paul Folino, had resigned in response." This story went viral and led to the market trading the company's shares as the price decreased. As a result of the fake press release, Emulex lost $2.2 billion and innocent investors in the market lost over $110 million. Despite subsequent news that this attack was proliferated by a community college hacker and the company was actually fine, the damage had already been done. Criminals also hack peoples' information to distribute amongst themselves in their own market.

The Deep Web, something that very few people know about, is the underground of the World Wide Web. It is a place where criminals interact and transact. The Deep Web is five hundred times larger than the surface of the Internet that we use.

"As a result, when you search Google, you are only seeing 0.03 percent (one in three thousand pages) of the information that actually exists and would be available online if you knew how to get it." The Internet sources that we use are essentially the tip of the iceberg. There is a vast amount of information on the web that is unknown to the general population. The Deep Web is where hackers, gangsters, terrorists and other criminals go to connect and conduct their illegal activities. The Deep Web is the home to illegal and horrific criminal transactions including pirated content, drugs, counterfeit currency, stolen luxury goods, stolen cards and accounts, identity theft, documents, weapons, hit men, child sexual abuse images, human trafficking, human organ trafficking, and live child rape. Innocent peoples' personal information are collected, stored, and sold on the Deep Web. Once your system is hacked, you are subjected to an invasion of privacy on an entire other level. Numerous criminals on the Deep Web will analyze your information and will transact to purchase it. Once you are hacked, there are numerous hands that hold your information and you have no idea who those hands belong to, where they are, and what they can do with the information they have.

The Surveillance Economy

Criminals and hackers are not the only people who have access to and exploit our information. Data brokers subject us all to invasions of privacy. Data brokers are entities that are able to collect information about people from numerous sources including Internet service providers, credit card issuers, mobile phone companies, grocery stores, and our online activities.

Acxiom, one data broker, has in its data banks approximately ninety six percent of American households. "Each profile contains more than fifteen hundred specific traits per individual, such as race, gender, phone number, type of car driven, education level, number of children, the square footage of his or her home, portfolio size, recent purchases, age, height, weight, marital status, politics, health issues, occupation, and

right- or left-handedness, as well as pet ownership and breed." Data brokers' goal with this information is to provide behavioral targeting, or predictive targeting, of your life. In other words, "this means understanding you with extreme precision so that data brokers can sell the information they aggregate at the highest price to advertisers, marketers, and other companies for their decision-making purposes." After a data broker gathers and groups your information into profiles of the similar sort, the data broker sells your profile to credit card issuers, retail banks, telecommunications companies, and insurers.

Why do data brokers sell our information to other entities? The analysis of our information "allows companies to find prospective customers with much higher degrees of accuracy and at greater value than previously possible." Goodman explained that when you search for something online and purchase another related item in a store, that information is logged and sold. As a result from this behavioral analysis, other companies can advertise their products to you based upon what you appear to be interested in, making that information valuable. While this initially seems to be beneficial and convenient to us as consumers, the digital trail that we leave behind is collected without our knowledge by a variety of entities (both legal and illegal) and can be used in ways that cause us harm. Goodman illustrates many examples of how data surveillance can result in privacy risks and other unpleasant surprises.

In one instance, a father discovered that his high school daughter was pregnant through information provided by his local Target store. Target had begun to send to the father's house coupons for baby clothes and apparel addressed to his daughter. Target found out that the father's daughter was pregnant before he did. Through its algorithms, Target aggregated the daughter's purchase history from its store and matched them with statistics purchased from data brokers about individuals who matched the purchases of the daughter. Through this, Target would advertise to consumers products they might be interested in for the purpose of securing them as customers.

Phone applications also collect your information. Free dating applications such as Tinder and OkCupid ask for answers to personal questions presumptively to help the user find a compatible match. After filling out information like how many partners you have had, your religion, and your views on abortion, OkCupid shares this information with numerous companies including ad firms, data brokers, and marketers. Dating apps are but one example out millions of applications that we can use that gather and sell our information.

We view ourselves as the consumer but we are actually the product that is being sold. We never think twice before we sign terms of agreements and use free products like Google and Facebook. Have you ever stopped to wonder why services like Google and social media sites are available for free? "A less altruistic explanation might be that each and every one of [these] products was created with the specific intent to trick, cajole, and coax users to reveal an ever-increasing volume of data about themselves and their lives." In return for their services, we unknowingly give them information about ourselves. Gmail was created to gain access to your personal and professional contacts in order to find new insights to offer to advertisers. Google Maps can track the places where you have been. Then, in 2012, Google announced it was merging all of its data across all of its various products and services. The result: all of your searches from the different services you used from Google, which were originally held separately, have been put together to create a unified, detailed picture of you and everything you do across all of its products.

Facebook also engages in selling our information to advertisers. "Facebook is a marketer's dream. Advertisers know every last intimate detail about a Facebook user's life and can thus market to him or her with extreme precision based upon the social graph Facebook has generated." Facebook has provided an avenue where people talk about themselves, disclosing intimate information details like relationships, sexual

orientation, purchases, photographs, religion, and news interests. Facebook has been sued frequently for issues pertaining to intercepting users' private messages and sharing that data with advertisers. Google and Facebook are but two examples amongst a broad range of companies that provide free services in exchange for obtaining your personal information. What is concerning is what these companies are doing with your information and who and where your personal data ultimately ends up being distributed.

Unfortunately, data brokers are often poor keepers of our information. The world of organized crime know that data brokers store vast amounts of information and can be lucrative targets. Between 2002 and 2003 over "1.6 billion customer records were stolen from Acxiom and its clients." Even worse, in 2013, "the data broker Experian mistakenly sold the personal data of nearly two-thirds of all Americans to an organized crime group in Vietnam. The epic fraud meant that the Social Security numbers of 200 million Americans became available to thieves around the world." Experian had failed to diligently check the entity that they were selling our information to because they were hypnotized by the amount of money that the unknown organization had offered. Infuriatingly, this was done at the expense of innocent American citizens' privacy.

Surviving Progress

It may seem that all of these risks should deter us from the use of technology. "The problem of course is not that technology is bad but that so few understand it. As a result, the computer code that runs our planet can be subverted and used against us by those who do." In order to maintain the security of our information with the rapid growth in technology Goodman emphasizes the importance of taking affirmative actions in understanding and regulating technology.

Goodman says, "[w]e need to help companies understand that it is in their long-term interest to write more secure code and that there will be consequences for failing to do so. As things stand today, the engineers, coders, and companies that create today's

technologies have near-zero personal and professional responsibility for the consequences of their actions." Given that software is the engine that runs the global economy, society must be able to hold the software industry accountable for their actions. Goodman says that a public debate is necessary to identify the causes of our technological insecurity. Further, we should demand changes in regulation to remove many companies' unconscionable protection from injury suits simply due to their terms of services. If this impediment is removed, individuals who have had their information exploited can seek recourse from the companies who misappropriated their information. Further, the threat of these suits will likely prompt companies to increase the security of the data they collect and improve their discretion in distributing this information to other entities.

The current state of our Internet is due to the type of market that we created. "The fallen state of our Internet is a direct... consequence of choosing advertising as the default model to support online content and services." Goodman discusses that while it may be impossible to live without connection to technology, a system can be designed to provide more protection to the user. Goodman suggests the possibility of adopting Europe's system, where there are limitations on what data companies can store about us and how long they can keep that information before being required to delete it. This is a more consumer-friendly model that emphasizes the importance of privacy as a fundamental right. Goodman explains that Europe's system adjusts the balance of power between individuals and Internet firms and more effectively protects the public from having their information leaked to criminals.

The use of two-factor authentication is an additional way that we can provide protection to our information. Two-factor authentication "combines your user name and password with something you have such as a... mobile phone." When a user goes to access their account, the company would require a second authentication, sent to your phone, in order for you to gain access to one of your accounts. "Thus even if a hacker

cracked your bank account, social media service, or social media profile, he would still need access to your phone and text message, something he would be unlikely to have [if you and the hacker were in different locations]." This method would be effective due to the amount of virtual crimes that are committed. If a second layer of authentication were required before accessing a user's account, it would decrease the likelihood that the hacker gains access to the user's information.

The use of encryption would also provide additional protection to our information. Today, the majority of data is unencrypted and in plain text. Without encryption, anybody who gains access to this data has the ability to read it. It is critical that society increases the use of encrypted communication. Encryption would scramble our information, requiring a password to decode the information, rendering the information valueless to an outsider who does not have access, thereby providing us with protection.

Goodman also suggests that we should create a Manhattan Project for the cyber realm. Goodman notes that we currently are not serious about the threat that looms before us as were the individuals working on the Manhattan Project. "[W]e must surely recognize that the underpinnings of our modern technological society, embodied in our global critical information infrastructures, are weak and subject to come tumbling down through either their aging and decaying architectures, overwhelming system complexities, or direct attack by malicious actors."

The evidence about the threats we face on the Internet are prevalent and must be recognized. Goodman reiterates that, on a daily basis, cyberattacks disrupt our financial system, billions of dollars are stolen in intellectual property, military operations are leaked and obtained by foreign nations, and hackers collaborate amongst each other, sharing their methods about how to destroy our society through the use of hijacked technology. These dangers are imminent and it is unacceptable to simply accept this as an inevitable consequence of technology. Goodman suggests to recreate the Manhattan

Project for the protection of our information in the cyber realm by bringing together the greatest minds of our time from all sectors of society: computer scientists, entrepreneurs, hackers, scientific researches, venture capitalists, lawyers, law enforcement officers, and military and intelligence personnel. With these minds thinking together, the goal of protecting our information on the Internet can be accomplished.

Finally, more education and awareness is required to strengthen the technological literacy of the general public. We need to provide information about how to stay safe on the Internet and how to properly interact using technology. This must be taught to people of all ages and should be included in the education curriculum. Individuals must be able to understand the threats that exist and take responsibility to protect themselves as best they can.

Conclusion

The future is here and the technological threats to our information are imminent. In order to protect our information we cannot sit idly by. We cannot simply pray that we will not fall victim to our information being leaked because this threat is inescapable. Now is the time to identify the threats, educate society, and build an innovative technological infrastructure that can protect our information from these emerging dangers. *Future Crimes* is a call to action to mobilize the common citizen and take back control of the technology that we created. Although these technologies can be used for good, we must identify and minimize the dangers they pose.

The Internet of Things and Cybersecurity: What Does a Lawyer Need to Know

Christopher W. Folk[1]

Abstract

We live in an increasingly interconnected world with smartwatches, smartphones, Internet-enabled vehicles, wearable biometric devices, and implantable connected devices, to name a few. In this age, we have shifted from a world in which the exception used to be the connected device to a new paradigm, where the standalone device is now the exception. The realm of interconnected networked devices is known as the Internet of Things ("IoT"). In this IoT world, information and privacy concerns are raised to new levels as the number of devices we use multiplies, and their use becomes ubiquitous meaning that either a breach or a loss of a device could compromise copious amounts of personal and private data. In such a world where personally identifiable information ("PII") exists in multiple permutations across a vast array of devices and media, cybersecurity is of paramount importance. While reports of identity theft and financial harm are pervasive, the advent of implantable medical devices raises concerns far beyond merely exposing data to theft, for in the medical technology field a cybersecurity breach could result in loss of life. With the pervasiveness of connected devices we (as individuals) need to recognize the threats and vulnerabilities to our privacy and information. Similarly, companies must also identify, assess, and mitigate these risks in order to limit unauthorized access to information and the resulting legal exposure.

In order to understand why privacy and security are such an issue in the IoT, we must look to the origins of the Internet. At its inception, the Internet as we know it today

1 Syracuse University College of Law, J.D. expected 2017. M.S. in Computer Information Systems, 2004. Special thanks to Professor Kathleen M. O'Connor for her encouragement and assistance throughout the development of this note. To Joseph Abrenio, Vice President of Delta Risk, I am grateful for the externship opportunity, the friendship, and the topic guidance. Finally, a special thanks to my wife, Tiffany for her encouragement and patience during my re-entry into academia, and also to my children who have been supportive and understanding throughout this process.

was designed to foster research and communication between known, trusted persons who were sited at specific physical locations. That model has evolved into the world of IoT where trusted identities are now the exception and physical locations are either indeterminate or meaningless in terms of trust and authentication. The original Internet underpinnings had an inherent lack of baked-in security protocols and, therefore, protection of privacy requires the addition of cybersecurity protocols and processes. In order to understand how privacy and the IoT interact, we will discuss information with a focus on PII as well as electronic personal health information ("ePHI"). We will then examine the IoT and discuss the paradigm shift that has occurred as we have evolved into a highly-connected world. Furthermore, we will examine the security implications inherent with the IoT. Finally, we will examine how the Internet, cybersecurity, and IoT impacts a law firm's duty of care with respect to the use and protection of information.

INTRODUCTION

In an age where your information flows throughout the airwaves connecting all of your devices in the IoT, cybersecurity becomes of paramount importance. When information retained in your "smart" refrigerator related to the brands and quantity of items you purchase, store, and subsequently consume is downloaded and viewed without your consent there is a certain level of privacy concern. However, when a hacker is able to connect to an implantable pacemaker which is connected to the Internet and send or prevent shocks from being delivered to a patient's heart for a myocardial event, a cyberattack raises entirely different concerns. The victim's life, not just her finances and privacy are in play. As we move towards a completely interconnected world where we are always within a keystroke of information, the risks to our right to privacy (and liberty) are ever-increasing, and even physical-health and well-being are at risk. Consequently, all entities (within both the private as well as public sector) are going to have to

get serious about cybersecurity or risk not only the loss of protected information but also potentially, the loss of life.[2]

Cybersecurity encompasses knowledge, assessment, and action. Knowledge in the sense that one must understand where information is stored and what the vulnerabilities are for the data; assessment in that people must couple their knowledge of personal, sensitive information as well as the current threats to identify the key vulnerabilities; coupled with action where people address the identified vulnerabilities in order to strengthen the overall cybersecurity framework. This is not groundbreaking or revolutionary in any respect and cybersecurity has been an acknowledged issue that has been widely covered by the mass media especially in the past couple of years (i.e. the IRS breach, the OPM data breach, Wyndham Hotels, etc.)[3].

This article provides a historical perspective to help the practitioner understand why we face these security concerns, why the privacy concerns matter to a law firm, and what steps a law firm can take to protect firm and client data. Accordingly, we begin with an introduction to the Internet and the rationale behind its design and inception. From there we delve into understanding the component pieces of cybersecurity, namely the human component as well as the technological piece. Following that we define what comprises data and information and within these realms what information is personally identifiable or protected health information for which additional safeguards must be implemented. Our perspective encompasses the full spectrum of cybersecurity from identifying data, its vulnerabilities and gaining and understanding of how (and if) the vulnerabilities must be mitigated. This background information will introduce the concept of Internet-ubiquity a lá the IoT where everything around us, and, in fact, many of

---

2 *See* Eric G. Orlinsky et al., *Cybersecurity: A Legal Perspective*, 47 Md. B.J. 32, 35 (Nov./Dec. 2014).

3 *How the Breach of Tax Returns is Part of a Much Bigger Problem Facing Taxpayers OPM's Cybersecurity Chief Resigns in Wake of Massive Data BreachLessons to be Learned from Wyndham Hotels Data Breach*,

the future things within us operate in a fully connected environment. Within this topic, we will explore what if any differences exist between public and private entities and actors as well as addressing if there is a varying standard of reasonableness that differs depending on the type of PII or ePHI that is at risk.

For our purposes, PII relates to sensitive personal information that could be used to identify who you are, where you live, data about you that you would not publish to the world. Whereas ePHI is similar though this data is specific to your personal health, medical conditions, medical history, etc. In the penultimate section, we will examine the difficulties that cybersecurity introduces into the legal landscape, be it in the protection of client data, the risks of unsecured eDiscovery data, or simply in ensuring that public and private entities have leveraged the proper legal advantage so that they are protected in the event of a data breach or hack. Within this vital topic area, we will attempt to discern how to mitigate risk and avoid the complicated patchwork of data breach notification laws that are still implemented on a state-by-state basis. Finally, a brief conclusion and suggestions to remain abreast of this dynamic and rapidly evolving area will be proffered.

The origins of the Internet

In 1962, J.C.R. Licklider discussed the concept of an overarching "Galactic Network" in a series of memos. While the concept of a "galactic network" actually predated the Internet itself, this phrase has taken on new meaning with the movement to an IoT.[4] The Internet as we know it began as a special project by the Federal Governments and the Defense Advanced Research Projects Agency ("DARPA"). The revolutionary aspect of this project was that it culminated in the development of a network based on packet-switching versus the traditional use of circuit switching. By using packets versus fixed virtual circuits, the end nodes can re-instantiate themselves after a failure without

4 Barry M. Leiner et al., *Brief History of the Internet*, Internet Society (Nov. 15, 2015), http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet#JCRL62.

having to be cognizant of the connection states.[5] The network created by DARPA was known as the Advanced Research Projects Agency Network ("ARPANET").[6] At the time the ARPANET came into existence, and for several years thereafter, it had been theorized by Vint Cerf and Robert Kahn that no more than 256 networks would be necessary for the foreseeable future.[7] However, with the introduction of local area networks ("LAN")s, it soon became clear that the number of networks had been vastly underestimated by many orders of magnitude.[8] Along with ARPANET, several other network designs sprang up and were not necessarily compatible with one another, which in and of itself was a security feature. For example, Because It's There Network ("BITNET ") was developed to link academic mainframe computers, USENET was developed to link UNIX computers, while the National Science Foundation Network ("NSFNET") was proposed to serve higher education. The NSFNET required that the transmission control protocol/Internet protocol ("TCP/IP ") networking protocol be adopted and this became the de-facto standard and is the protocol upon which the modern Internet depends.[9]

The Internet was originally designed and purpose-built to connect a small group of trusted systems and users and was not originally intended for global use. At

---

5 David D. Clark, *The Design Philosophy of the DARPA Internet Protocols*, MIT Laboratory for Computer Sci. (1988), http://nms.csail.mit.edu/6829-papers/darpa-internet.pdf. (With virtual circuits, the end points needed to understand the connection state since this was a fixed type of service, whereas with the use of packets, the packet contains the necessary information and the source and destination are able to retransmit and reassemble packets even if an endpoint goes "down" and packets are lost).

6 *Id.*

7 Barry M. Leiner, et al., *Brief History of the Internet*, Internet Society, http://www.internetsociety.org/sites/default/files/Brief_History_of_the_Internet.pdf (last accessed Mar 23, 2016). This article discussed the memo that Vint Cerf and Bob Kahn developed the design specifications for what would eventually become TCP/IP. Kahn and Cerf chose 32-bit addressing schemes with the first 8 bits signifying the network and the remaining 24 bits available for hosts addressing since they believed that there would be no need in the foreseeable future to have more than 256 networks.

8 *Id.*

9 *Id.*

its inception, devices which were interconnected were personally authenticated and known amongst the handful of researchers. Consequently, what began as a small, trusted network where users and systems were known and authenticated through direct knowledge has grown into a massively interconnected system with more users and systems utilizing the network than even existed in the world when the ARPANET was first introduced.[10] However, with the advent of the computing age and the movement to ensure that every household has a computing device personal knowledge, of each device is neither practical nor possible.[11] Consequently, in a system designed to rely on trust and personal knowledge, when the number of devices being connected increases and we move towards an IoT, there are a number of inherent vulnerabilities in the Internet underpinnings, some of which will be discussed hereinafter.

The Domain Name System

While the local Post Office sorts and processes physical mail (information), in the Internet world, the Domain Name System ("DNS") performs a similar addressing and routing function for digital information. In the Internet, each networked device has a unique Media Access Control ("MAC") address and this is roughly analogous to a Zip+4 code coupled with a house address (including street, and house number). While the post office and mail carriers sort and deliver packages, DNS uses the numerical addressing system to sort and deliver packets from a sender address to the proper destination address. In order to effect this, it is necessary to translate human-readable language into machine-compatible code using a translation system. This is DNS and it is used to translate specific TCP/IP addresses which are comprised of octets, such as 128.230.146.40 into standard language that humans can readily remember and utilize

10 Craig Timberg, *Net of Insecurity: A Flaw in the Design*, The Washington Post (May 30, 2015), http://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/

11 Claudine Beaumont, *Bill Gates's Dream: A Computer in Every Home*, The Telegraph (Jun. 27, 2008), http://www.telegraph.co.uk/technology/3357701/Bill-Gatess-dream-A-computer-in-every-home.html.

such as "www.law.syr.edu."

Consequently, typing the address www.law.syr.edu into an Internet browser, the system must access a DNS server to translate the address from human-readable text into a specific (numeric) IP address. Consequently, this raises the possibility that a hacker could target the DNS server to modify the routing tables so that when a user attempts to go to a website they are instead redirected to a different site. From there, the hacker could either direct the user to a fake (spoofed) site where the hacker could capture a user's username and password, or the hacker could simply prevent a person from accessing a specific site, (similar tactics are sometimes employed to create distributed denial of service ("DDOS") attacks that prevent users from accessing websites.[12]

The Border Gateway Protocol

While DNS is analogous to the local post office, the Border Gateway Protocol ("BGP") is more like a large regional or national mail processing center. The regional mail processing centers take mail in and then process and sort for delivery to individual post offices. In the context of the Internet, BGP performs a similar function. The vast majority of users connect to the Internet through an Internet service provider ("ISP") which then connects to the Internet backbone. An ISP would be the larger carriers, such as AT&T, Time Warner, Charter Communications, etc. In order for ISPs to connect to the backbone and to each other, a system known as a BGP was developed.[13] Essentially this system operates like a post-office relay system, in that every data packet has a destination address and a return address to connect ISPs to one another. BGP relies on the truthfulness of the packet itself and does not perform any outside verification or authentication of from and to addresses. Consequently, one can simply "spoof" the destination or return address and cause the misdirection of packets. Therefore, while BGP is integral

12 Richard A. Clarke & Robert K. Knake, Cyber War: The Next Threat to National Security and What to do About it 77 (2010).

13 *Id.*

to packet-routing between ISPs it is highly susceptible to packet spoofing which could cause the redirection of a few packets or could be used to redirect entire packet streams from legitimate users to nefarious sites.

Lack of Internet Governance

Once ARPANET transitioned into what we now know as the Internet, it became an enormous system with interconnected devices which was largely ungoverned by formal rules and regulations. Consequently, *de facto* standards and industry forces have combined to adopt protocols and processes which are generally operated outside the auspices of federal or international oversight. As the Internet has expanded from the US to the international space, there have been many calls for international governance of the Internet.[14] Specifically, while the Domain name system is managed by the Internet Corporation for Assigned Names and Numbers ("ICANN"), this is not technically managed by any single entity or government.[15] Although ICANN was initially facilitated by the U.S. Department of Commerce ("USDOC"), the USDOC relinquished direct control over ICANN in 2009. However, ICANN continues to operate as a U.S. Corporation (incorporated in the State of California), and while it touts multi-stakeholderism, it is still largely believed to be a US-centric construct.[16] Consequently, ICANN is not truly an independent organization, and this becomes an issue since one of the perceived issues with ICANN is the fact that modifying or taking the domain name system offline could result in a global disruption in Internet traffic.[17] Most countries in the world are not comfortable with this much power and control over the Internet resting singularly within the United States.[18]

---

14 Milton L. Mueller, Networks and States: The Global Politics of Internet Governance, 10-11 (William J. Drake & Ernest J. Wilson II eds., 2013).

15 *A Quick Look at ICANN*, https://www.icann.org/en/system/files/files/quick-look-icann-01nov13-en.pdf.

16 , *supra* note 14, at 61-62.

17 , *supra* note 12, at 78.

18 The United States itself does not seem to share the same concerns as other global actors.

Lack of Encryption: The ubiquity of clear-text

The Internet is by design open and unencrypted. Most information transferred between your computer and other networked resources is done in a clear-text fashion, which means the information is easily and readily human-readable.[19] Packet sniffers, which are either hardware or software devices that sit within a network stream and essentially gather all passing packets, can be placed within the network and can snoop on all of the traffic traversing the network and any unencrypted data are human readable. Furthermore, the use of keystroke-loggers which capture every key pressed on a user's system can also be used to capture every single keystroke, and then transmit it to a remote user. These keystroke-logger devices can be self-contained within a USB drive or downloaded as malware. Once installed on a user's machine they capture every key press and then either save the data for later export or automatically upload. Where the connection between a computer and the physical keyboard is unencrypted, keystroke-loggers could capture everything in clear text and allow PII, ePHI, or username/password combinations to be obtained without the user's knowledge.[20]

Speed versus Security

ISPs compete with one another for customers, and the prevailing view amongst customers is that ISPs are measured in terms of their download and upload speeds; security is at best a tertiary concern. Therefore few, if any ISPs make any effort to inspect packets to ensure that viruses or worms are not being carried across their networks.[21] Not only are ISPs more concerned with upload and download speeds, but they have no incentive to perform deep packet inspection ("DPI"), or stateful packet inspection

---

19 Clear-Text merely denotes the use of standard characters and words; whereas encryption replaces characters and words with symbols and characters that must be decrypted before they can be read.

20 *Id.* at 80.

21 *Id.* at 81.

("SPI") for the purposes of detecting and preventing viruses or malware.[22] Consequently, self-replicating code, as well as phishing scams, are allowed across the networks with essentially no checks whatsoever. The focus of ISPs and Internet backbone providers is on speed and availability, rather than security and the welfare of an ISP's users. Consequently, ISPs use DPI but only to enable them to provide Quality of Service ("QOS") based on content type (for example, voice over IP ("VOIP") services that may receive higher priority over file transfer protocols).[23] It seems that users are typically more concerned with dropped calls than with data breaches.

Decentralized Design

The Internet evolved from the ARPANET, which was designed to work independently of any global control framework. Consequently, the actual design of the Internet requires that security is layered on rather than integrated into the underlying protocols.[24] Specifically, the overarching guiding principles behind the original ARPANET design were:

- Each network should stand on its own and require no internal changes to connect to the Internet.
- Communications operate on a best-effort basis. If a packet does not reach the final destination, the source should retransmit.
- Black boxes would be used to connect networks to each other (these are now referred to as gateways and routers). The black boxes should not retain any information related to the packets that pass through them.
- There should be no global control of the network.[25]

22 Angela Daly, *The Legality of Deep Packet Inspection*, 14 Int'l J. Comm. L. & Pol'y (2010), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1628024.

23 *Id.*

24 The "layering" here refers to the fact that one has to add something to the standard network and TCP/IP in order to make data secure. One approach is to move to a secure border with edge-devices that restrict inbound and outbound packets, another approach is to encrypt communication channels and use tunneling (e.g. Virtual Private Networks); whereas there is also a data-centric model where the focus is on the data and subsequently data is encrypted and while the network is still recognized as a point of vulnerability less effort is devoted to the network and resources are instead directed to the real jewels - the data itself.

25 *See* Clark, *supra* note 5, at 112.

Additionally, TCP/IP was known to be unsecure however it was reasoned that TCP/IP was designed for small networks and it was more important that the protocol is fast rather than secure. Since the initial network involved routers that were housed in secure locations in academic laboratories and government agencies, it was theorized that the transmission lines between routers or points on the network could simply be encrypted, which would be easier and faster than creating a secure transmission protocol.[26]

What is cybersecurity?

While the term cybersecurity has been used extensively in headlines recently, it is important to take a step back and consider what the term really means. The International Telecommunication Union ("ITU") defines cybersecurity as the following:

Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment.27

While the National Institute for Cybersecurity Careers and Studies ("NICCS") defines cybersecurity as: "an activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification or

---

26 , *supra* note 12, at 43-44.

27 *Definition of Cybersecurity*,, https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx (last visited Mar. 16, 2016).

exploitation."[28] While this is general enough to cover most of the nuances of cybersecurity, the definition does little, if anything to explain what cybersecurity really means for a private or public actor. To understand what cybersecurity actually is, it may be helpful to consider some of the most common cyberattacks. Nine attack types comprise over 90% of the top threat patterns: (1) malware designed to overtake systems; (2) insider privilege misuse; (3) physical theft or loss; (4) web application attacks; (5) DOS attacks; (6) cyber espionage; (7) point-of-sale intrusions; (8) payment card skimmers; and (9) user error (such as sending a communication to an improper addressee).[29]

For our purposes, if we define cyber assets to include access, authorization, use, and dissemination of any and all electronic information, then cybersecurity is the framework within which the electronic assets are: (1) validated (e.g. ensuring that data is not modified without logging), (2) available (authorized users are able to access the appropriate data), and (3) confidential (the ability to access data varies based on prescribed user access needs).[30] We can break this down further into the human and the technological elements. On the human side of the equation, education is perhaps the most effective tool used to enhance overall cybersecurity. Within this realm, it is vital to ensure that users understand what the issues and goals of cybersecurity are so they can appreciate why they are being asked to do things such as create complex passwords, change their passwords every 90 days, or begin to use two (multi) factor authentication.[31] Similarly, one of the largest and most effective threats involves the use of spear phishing campaigns where "official" looking e-mails are sent to users who are asked to respond with their login credentials. Confronting these threats using education, attacking the human side of

28 *Glossary*, , https://niccs.us-cert.gov/glossary#letter_c (last updated Mar. 31, 2017).

29 Warwick Ashford, *Most Cyber Attacks Use Only Three Methods, Verizon Breach Report Shows*, (Apr. 23, 2014), http://www.computerweekly.com/news/2240219278/Most-cyber-attacks-use-only-three-methods-Verizon-breach-report-shows.

30 , *supra* note 27.

31 Michael Hill, *The 'Human' Side of Cybersecurity*, infoSecurity, http://www.infosecurity-magazine.com/blogs/the-human-side-of-cybersecurity (last visited Mar. 17, 2016).

the equation, is likely far more efficient and effective than taking a purely technological approach.[32] On the technology side tools include layering on security to existing products, such as DNS, BGP, and encrypted transmissions, as well as encrypting data (both in-flight and at-rest).[33]

What constitutes PII and ePHI?

This paper frequently uses the terms PII and ePHI although they are not self-explanatory. According to the Office of Management and Budget ("OMB"), PII is "information which can be used to distinguish or trace a person's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."[34] Whereas, the U.S. Department of Health & Human Services defines Electronic Protected Health Information ("ePHI") as "all individually identifiable health information a covered entity creates, receives, maintains, or transmits in electronic form."[35]

Essentially, PII is a broader, more encompassing term, within which ePHI falls. However, given the fact that ePHI is often governed under the Health Information Privacy Protection Act ("HIPAA"), the two terms are broken out based on the type of information that is being discussed. If you view PII as the base level, then ePHI is analogous to PII+ and the "+" denotes that ePHI is subject to additional regulations under HIPAA as well as the Health Information for Economic and Clinical Health ("HITECH") Act.[36]

---

32 *Id.*

33 In-flight data refers to data that is moving (in-motion), such as when packets are being sent on the Internet, whereas data at-rest could be thought of as stored data, such as data on a hard drive, or a USB stick that is sitting idle and not being accessed.

34 (May 22, 2007).

35 *Summary of the HIPAA Security Rule*, (Nov. 15, 2015), http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html.

36 *Id.*

The Internet of Things

Scientist Kevin Ashton first used the term "Internet of things" back in 1999, while giving a presentation about radio frequency identification ("RFID") at Procter & Gamble.[37] This IoT universe is now becoming a reality, with smartphones that harness vastly greater computing resources than existed in the mainframe computers back in the 1970s, with smart watches, wearable technology, implanted health monitoring devices, smart appliances, self-driving vehicles, drones, smart TVs, in-utero baby monitors, among other devices.[38] We live in an increasingly connected world where data flows all around us and from a seemingly infinite number of devices. In the wearable technology arena alone, it is estimated that the market for these types of devices is going to exceed $34 billion.[39]

The IoT and Cybersecurity Considerations and Implications

As our connected world has evolved from university researchers with physical links between machines to a vast array of computing devices with embedded networking capabilities, cybersecurity has become more and more important. So too, as we continue to migrate towards an IoT, it becomes clear that certain IoT devices open us up to risk far beyond the mere loss of data.

IoT: Wearable technology and implantable medical devices – risks range from ePHI breaches to death-by-remote access.

Wearable technology and medical devices appear to be the new frontier of

37 Kathleen Aguilar, *Getting up to Speed on the Internet of Things*, 26, 28 (2015), http://www.accdocket.com/vl/public/ACCDocketArticle/loader.cfm?csModule=security/getfile&pageid=1410594&page=/docket/articles/resource.cfm&qstring=show=1410594&title=Getting%20Up%20to%20Speed%20on%20the%20Internet%20of%20Things%20&recorded=1.

38 *Id.* at *28.

39 Paul Lamkin, *Wearable Tech Market to be Worth $34 billion by 2020*, (Feb. 17, 2016), available at http://www.forbes.com/sites/paullamkin/2016/02/17/wearable-tech-market-to-be-worth-34-billion-by-2020/#1ca4a7f63fe3.

IoT devices. Currently, a wide array of devices, including stationary, wearables, implantables, or ingestibles allow individuals as well as providers to monitor a variety of biometric indicators as well as real-time monitoring (for instance to evaluate the efficacy of current prescriptions, or the efficiency of a pacemaker, etc.).[40] Consequently, these devices are designed with remote access capabilities for administration and monitoring. The ability to remotely access and control these devices opens up the potential for nefarious access either to pilfer information or to impose more dire impacts such as over administering insulin or delivering shocks when an individual is not undergoing a myocardial event - each of these cases could potentially induce death and the cause might be traced to a faulty device rather than a "hack".[41] For instance, the National Institute of Standards and Technology ("NIST") is revising its original guidance on devices such as wireless infusion pumps.[42] NIST's new white paper comes on the heels of a warning issued by the Food and Drug Administration ("FDA") which urges healthcare organizations to discontinue using the Hospira Infusion System due to cybersecurity vulnerabilities.[43] As privacy and security attorney Kirk Nahra says, medical devices carry a much different risk in that it isn't merely information that is at risk but rather the viability of an actual living person - thus medical devices cyber vulnerabilities could have far more dire consequences than other IoT devices.[44] An additional challenge facing medical devices

40 Mathias Cousin, Tadashi Castillo-Hi & Glenn Snyder, *Devices and Diseases: How the IoT is Transforming MedTech*, (Sep. 11, 2015), http://dupress.com/articles/internet-of-things-iot-in-medical-devices-industry/.

41 Marc Goodman, *Who Does the Autopsy? The Criminal Implications of Implantable Medical Devices*, Slate (Mar. 17, 2015), http://www.slate.com/articles/technology/future_tense/2015/03/implantable_medical_devices_hacking_who_does_the_autopsy.html.

42 Marianne Kolbasuk McGee, *Why NIST Is Revising Infusion Pump Cybersecurity Guidance*, (Mar. 7, 2016), http://www.healthcareinfosecurity.com/interviews/nist-revising-infusion-pump-cybersecurity-guidance-i-3094?rf=2016-03-09-eh&mkt_tok=3RkMMJWWfF9wsRonvq3Kd%2B%2FhmjTEU5z16esrWKC0hIkz2EFye%2BLIHETpodcMTcFqNb%2FYDBceEJhqyQJxPr3FKdENwM10RhPhDw%3D%3D.

43 Marianne Kolbasuk McGee, *FDA: Discontinue Use of Flawed Infusion Pumps*, (Aug. 3, 2015), http://www.healthcareinfosecurity.com/fda-discontinue-use-flawed-infusion-pumps-a-8449.

44 *Id.*

is the traditional development cycle, in which it may take ten years or more in order to gain FDA approval. Thus, while cybersecurity is acknowledged across the industry as an important issue, it may be several years before a cybersecurity focus can be applied to medical devices in the marketplace.[45]

Additionally, there are some competing interests at play since the data and control of medical devices requires that they have embedded connectivity; thus, while manufacturers are trying to address cybersecurity they are also faced with the need to make their devices highly compatible so that the information from the devices can be leveraged by a wide array of healthcare providers.[46]

IoT, PII, ePHI -- What is a lawyer to do?

Moving from consumer and manufacturers to the legal world, we must now consider, with IoT, PII, and ePHI, what lawyers must be cognizant of, and how should they protect themselves and their clients? With the advent of electronic Discovery ("eDiscovery") and the rising sophistication of both state and non-state hackers, law firms have been, and will continue to be, targeted.[47] The issue being that, consumers as well as companies are beginning to take cybersecurity seriously and consequently, hackers understand that trying to effect a data breach from a bank, for instance, could be extremely difficult. However, if a bank were involved in litigation and the bank's law firm had possession of copious amounts of data, the law firm with likely far lower levels of cybersecurity becomes a logical target. So too, in the case of hacktivists where a law firm may be involved in the defense of persons that are themselves the target of activists, this could result in the law firm becoming a target as well. With respect to law firms, it seems that hackers view these as having lax cybersecurity and it is estimated that one of

45 *Id.*

46 Cousin et al., *supra* note

47 Keith Lee, *Is Your Law Firm a Target for Hackers? (Spoiler: Yes)*, (Mar. 5, 2015, 1:16 PM), http://abovethelaw.com/2015/03/is-your-law-firm-a-target-for-hackers-spoiler-yes/.

the most problematic attacks facing law firms is spear phishing (an example of an e-mail spear phishing attack would be faking the sender address so that an e-mail appears to come from a Senior Partner in the Law Firm, requesting that the lawyer clicks on a link and change their password due to a potential security breach, before the link redirects the user and allows the attacker to capture the username and password).[48] The focus of this section then will be on discussing some data breach cases and then consider the legal liability of a law firm and conclude with the law firm's standard of care with respect to data.

Legal Liability[49]

What is the legal standard applied to lawyers regarding the safeguarding of electronic client data? Unfortunately, this fundamental question is far from settled as there is currently little guidance on this new area of the law. However, two recent cases have provided a basic litmus test where there is an inadvertent data disclosure. For instance, in *Victor Stanley, Inc. v. Creative Pipe, Inc.*, defense attorneys inadvertently disclosed privileged information to the plaintiff's attorneys during the discovery phase of the litigation.[50] After learning of their mistake, the defense sought assistance from the court in an attempt to retrieve the data and identify any data that was privileged in order to preserve client confidences.[51]

When deciding the issue, the Court outlined a five-factor balancing test to be applied to determine whether the inadvertent production of attorney-client privileged information waives the attorney-client privilege: (1) the level of reasonableness of the

48 *Id.*

49 This Section is taken extensively from the author's previous work conducted as the basis for the underlying research of this paper. This is included here with permission of Delta Risk. This work became a viewpoint article and is available at http://www.delta-risk.net/s/Oct2015DeltaRisk_LawFirmDutyProtectConfidentialData_07102015_v10.pdf.

50 Victor Stanley, Inc. v. Creative Pipe, Inc.,

51 *Id.*

precautions taken to prevent inadvertent disclosure, (2) the aggregate number of inadvertent disclosures, (3) the depth of the disclosures, (4) amount of delay (if any) between disclosure and attempts to rectify same, and (5) the overriding interests of justice. Applying the above, the Court determined that defense counsel's inadvertent disclosure had eviscerated the attorney-client privilege.[52]

The *Kyko Global, Inc. v. Privthi Info. Solutions* case involved an unsuccessful attempt to delete privileged electronic data from a computer hard drive that was to be provided to opposing counsel.[53] Specifically, the defendants reformatted the computer hard drive and installed a new operating system in an attempt to delete any existing data.[54] Here, the court applied a more detailed five-factor balancing test when deciding whether or not the confidential client data would maintain its privileged status: (1) were the precautions reasonable; (2) how much time was required to mitigate the error; (3) what was the overall breadth and depth of discovery; (4) what was the scope of the disclosure; and (5) what, if any, impact did this have on the fairness of the proceeding.[55] Ultimately, the court decided that the act of formatting a hard drive and re-installing an operating system to delete any existing data was a reasonable precaution and held that the recovered information would remain privileged. [56]

With regard to external breaches, law firms are increasingly being targeted. One such example is the 2012 attack on the law firm of Puckett & Faraj where hackers extracted sensitive client files from the firm and posted the files online.[57] This breach had

52 *Id.* at 259.

53 Kyko Global, Inc. v. Privthi Info. Solutions, Ltd., NO. C13-1034 MJP, 2014 U.S. Dist. LEXIS 81132, at *8-12 (W.D. Wash. June 13, 2014) (*citing* Sitterson v. Evergreen Sch. Dist. No. 114, 147 Wash. Ct. App. 576 (2008)).

54 *Id.*

55 *Id.*

56 *Id.*

57 Matthew Goldstein, *Citigroup Report Chides Law Firms for Silence on Hackings*, (Mar. 26, 2015), *available at* http://www.nytimes.com/2015/03/27/business/dealbook/citigroup-report-chides-

a tremendous impact on this small firm, which was unable to remain viable once their reputation took this very public hit.[58] The aforementioned cases demonstrates that a law firm's exposure is not limited merely to what is lost or to a breach of client data, but rather the firm's viability may be dealt a fatal blow if a firm suffers a data breach and is unable to allay consumer confidence issues. To a law firm, confidentiality is sacrosanct and once violated it may be impossible for a firm to regain the trust of their clients. This significant breach ultimately resulted in the dissolution of the law firm - (Puckett is now Director of Special Inquiries Division with the Naval Inspector General, whereas Faraj has a private practice in the Chicago area) a dire indicator of the potential ramifications of a public breach.[59]

Another notable case involved the firm of Gipson, Hoffman & Pancione, which filed a software piracy lawsuit alleging that the Chinese government colluded with Green Dam and stole their client's intellectual property and then distributed over 56 million copies of the infringed software throughout China.[60] Soon thereafter, the firm was subjected to targeted cyber attacks in the form of spear phishing e-mails, which were designed to appear as though originating from within the firm and contained Trojans.[61] Fortunately, Gipson, Hoffman & Pancione's IT department had taken a proactive approach and users were aware that phishing e-mails and Trojans were an issue that they needed to be cognizant of.[62] Consequently, while the attacks were initiated they proved

---

law-firms-for-silence-on-hackings.html?_r=0.

58 *Id.*

59 , http://www.farajlaw.com (last visited Mar. 20, 2016); Neal Puckett, , https://www.linkedin.com/in/nealpuckett (last visited Mar. 20, 2016).

60 Goldstein, *supra* note 57.

61 Robert McMillan, *Law Firm in Green Dam Suit Targeted With Cyber-Attack*, (Jan. 13, 2010), *available at* http://www.nytimes.com/external/idg/2010/01/13/13idg-law-firm-in-green-dam-suit-targeted-with-cyber-attac-95001.html.

62 *Id.*

to be unsuccessful.[63] Here IT passed on key knowledge to users and because of this, the firm was relatively unscathed by what otherwise could have been a devastating and crippling attack.[64]

Finally, in 2014 after a top-secret document that was obtained by Edward Snowden was released, it was widely reported that the National Security Agency ("NSA") and its Australian counterpart had been monitoring communications between the Mayer Brown law firm and Indonesian officials (clients of the firm).[65] Here, the Mayer Brown law firm was representing Indonesian officials while the Indonesian Government had an ongoing trade dispute with the United States.[66] This revelation forces law firms to evaluate whether the use of electronic communication involving sensitive information with overseas clients should be shelved in favor of in-person meetings and standard correspondences.

The Law Firm's Standard of Care

As evidenced above, law firms must appreciate that the digital domain is far different from the traditional realm of paper files. Securing electronic data is far more challenging than locking a file cabinet. As the *Kyko* case demonstrates, attorneys and legal staff must act "reasonably" when collecting, transfer, storing, and purging electronic data. Court's will look at the totality of the circumstances in order to evaluate whether or not this standard has been met. Accordingly, law firms must ensure that their lawyers and staff have adequate training and supervision with regard to the safeguarding of electronic data.

---

63 *Id.*

64 *Id.*

65 James Risen and Laura Poitras, *Spying by N.S.A. Ally Entangled U.S. Law Firm*, (Feb. 15, 2014), *available at* http://www.nytimes.com/2014/02/16/us/eavesdropping-ensnared-american-law-firm.html?_r=0.

66 *Id.*

Professional Responsibility and Ethical Considerations

In addition to the legal requirements governing client electronic data, lawyers must also consider emerging ethical regulations. The American Bar Association ("ABA") Model Rules 1.1, 1.6, and 5.3 specifically address confidential client electronic data.[67] ABA Model Rule 1.1, which requires lawyers to provide competent counsel now extends that competency to the use of technology.[68] Under the comments to ABA Model Rule 1.1, a lawyer is expected to stay abreast of changes in the law and its practice "including the benefits and risks associated with relevant technology."[69]

Additionally, Rule 1.6 expressly outlines factors that may be evaluated to determine what constitutes competent actions to preserve confidentiality:

1. The sensitivity of the information,
2. The likelihood of disclosure if additional safeguards are not employed,
3. The cost of employing additional safeguards,
4. The difficulty of implementing the safeguards,
5. The extent to which the safeguards adversely affect the lawyer's ability to represent clients.[70]

Model Rule 1.6 indicates that an attorney does not violate Rule 1.6 so long as the unauthorized access to, or disclosure of information occurs where the lawyer took reasonable efforts with respect to each of the five steps outlined above.[71] The bottom line is, law firms must evaluate their existing safeguards and ensure that they are "reasonable" in light of the five factors above.

A lawyer's burden does not end with Rule 1.6. As cloud-based data storage is becoming more prevalent in the law firm environment, the ABA has modeled additional

---

67 Model Rules of Prof'l Conduct R. 1.1 cmt. 8; R. 1.6 cmt. 18; R. 5.3 cmt. 3 (2013).

68 R. 1.1 cmt. 8 ().

69 *Id.*

70

71 *Id.*

ethical rules to address this increasingly popular method of data storage.[72] As of the date of this writing, twenty states have issued formal opinions or advisories related to the permissibility of cloud storage and the appropriate standard of care.[73] ABA Model Rule 5.3 dictates that cloud-based storage may be viewed in the same light as a "[n]onlawyer outside the firm" and is subject to the following guidelines: (1) reasonable efforts must be made to ensure the cloud services provider is compatible with a lawyer's professional obligations; (2) an evaluation must be made of the services being provided; (3) the provider's stated or understood terms with respect to the protection of client information; and (4) the legal and ethical guidelines associated with the specific jurisdictions within which the services will be performed.[74]

As the ABA Model Rules continue to evolve to incorporate the increased use of technology amongst lawyers and law firms, so too will the model rules in individual states (many states have either adopted or have proposed the adoption of the updated 2013 ABA Model Rules 1.1; 1.6; and 5.3).[75] A number of noteworthy state ethics opinions have considered a lawyer's ethical obligations to safeguard client data. In *Cal. State Bar Standing Comm. On Prof'l Responsibility and Conduct Formal Op. No 2010-17976*, six steps were outlined for an attorney to follow when using technology to store or transmit confidential client information: (1) assess the level of security in a specific technology and determine if reasonable precautions could positively impact the level of security, (2) gauge the legal liability that exists with respect to a third party that accesses, intercepts, or exceeds their authorized privileges with respect to electronic data, (3)

72

73 *Cloud Ethics Opinions Around the U.S., available at*

74

75 *27 States Have Adopted Ethical Duty of Technology Competence*, (Mar. 8, 2017), http://www.lawsitesblog.com/2015/03/11-states-have-adopted-ethical-duty-of-technology-competence.html.

76 Cal. State Bar Comm. on Prof'l Responsibility and Conduct, Formal Op. 2010-179.

determine the level of sensitivity of the data, (4) analyze what impact an inadvertent disclosure of data would have on a client, (5) assess whether there are any urgent or exigent circumstances, and (6) has the client delivered specific instructions or protocols with respect to data access.[77]

Similarly, in *AZ State Bar Op. No. 05-04*, the Arizona State Bar categorized electronic data into three distinct categories: (1) stolen electronic information; (2) inadvertently disclosed information, and (3) lost, or destroyed electronic information. [78] Essentially, the Arizona State Bar opined that precautions must be taken to prevent the theft of confidential communications.[79] While in the case of inadvertent disclosures, the onus is on the lawyer to either become familiar with hardware and software technology to properly assess their security and protection measures or alternatively to engage with outside experts to do so. Similarly, in the case of the loss or destruction of electronic data, a lawyer must either achieve the relevant levels of competence to understand the technological issues or must utilize outside experts.

The New York, and New Jersey State Bars have issued ethics opinions that essentially require the use of reasonable care to safeguard client data, whether it be data at rest, in-flight data, or data which resides with a third party.[80] Whereas Pennsylvania went a little further and outlined a comprehensive checklist that law firms may follow in order to exercise reasonable care.[81] Additionally, Pennsylvania extended ABA Model Rule 1.15 (Safekeeping property) to include files, information, and documents stored electronically.[82]

---

77 *Id.*

78 Ariz. State Bar Ethics, Formal Op. No. 05-04 (2005).

79 *Id.*

80 *See*

81

82 *Id.* Reasonable care for "cloud computing" may include:

1. Backing up data to allow the firm to restore data that has been lost, corrupted, or accidentally deleted,

As the ABA and individual states continue to grapple with safeguarding electronic data, rules and opinions will continue to be updated. As such, an attorney's legal and ethical obligations to safeguard electronic data will remain dynamic as technology evolves. This ever-changing dynamic will force firms to decide whether or not to invest in-house resources outside the traditional "billable" hours or whether a more prudent course of action is to leverage industry experts to provide outside cybersecurity services for financial efficiencies.

Electronic Personal Health Information (ePHI)

HIPAA coupled with the Health Information for Economic and Clinical Health

---

2. Installing a firewall to limit access to the firm's network,
3. Limiting information that is provided to others to what is required, needed, or requested,
4. Avoiding inadvertent disclosure of information,
5. Verifying the identify of individuals to whom the attorney provides confidential information,
6. Refusing to disclose confidential information to unauthorized individuals without client permission,
7. Protecting electronic records containing confidential data, including backups, by encrypting confidential data,
8. Implementing electronic audit trail procedures to monitor data access,
9. Creating plans to address security breaches including the identification of persons to be notified in event of a breach or suspicion of a breach,
10. Ensuring the provider:
    a. Explicitly agrees it has no security or ownership interest in the data,
    b. Has an enforceable obligation to preserve security,
    c. Will notify the lawyer if requested to produce data to a third party, and provide lawyer with the ability to respond to the request before the provider produces the requested information,
    d. Has technology built to withstand a reasonably foreseeable attempt to infiltrate data, including penetration testing,
    e. Includes in its "Terms of Service" or "Service Level Agreement" an agreement about how confidential client information will be handled,
    f. Provides firm with right to audit provider's security procedures and obtain copies of any security audits performed,
    g. Will host the firm's data only within a specified geographic area. If hosted outside the US, the law firm must determine that the hosting jurisdictions has privacy laws, data security laws, and protections against unlawful search and seizure that are minimally as rigorous as those of the US and PA,
    h. Provide a method of retrieving data if the lawyer terminates use of the SaaS product, the SaaS vendor ceases business operations, or the service otherwise has a break in continuity, and
    i. Provides the ability for the law firm to get data "off" of the vendor's or third party data hosting company's servers for the firm's own use or in-house offline backup

("HITECH") Act serve as frameworks for security protocols and procedures for those using or accessing ePHI. Where a lawyer or law firm reviews medical records or accesses ePHI they may be held to the HIPAA standard as "business associates".[83] Law firms are subject to the standard industry guidelines when they perform functions, such as reviewing medical records, and may be found to be "business associates" under HIPAA.[84] Consequently, those that provide legal services that require the use or review of ePHI must implement additional safeguards lest they be subjected to additional breach notification requirements as well as the potential for fines, penalties, and the possibility of an on-going audit and compliance program imposed by the Federal Trade Commission ("FTC") which could persist for up to twenty years.[85]

Understanding and implementing HIPAA and HITECH data controls is a two-prong process: 1) the firm must determine whether its use of and access to the ePHI renders that firm a business associate under HIPAA; and 2) whether the firm has performed a risk assessment such that it can establish compliance with ePHI controls under HIPAA and HITECH.[86] Under the first prong, where a firm requires access to ePHI in a suit (e.g. medical malpractice), the firm will be held to be a business associate.[87] The second prong then requires that the firm must perform a risk assessment to evaluate its current security practices and controls with respect to electronic information in order to ensure compliance.[88] The HIPAA privacy rule mandates that covered entities must control access to and the use of ePHI; whereas the security rule requires that ePHI be protected by a business

---

83 Timothy J. Toohey, *Beyond Technophobia: Lawyer's Ethical and Legal Obligation to Monitor Evolving Technology and Security Risks*, 21 Rich. J.L. & Tech 9, 17 (2015).

84 *Id.*

85 *Id.*

86 Sarah S. Murdough et al., *Omnibus Rule Implications for Law Firms as Business Associates*, 16-17, http://www.harmonie.org/user_documents/HIPAA_Omnibus_LawFirms1.pdf.

87 *Id.* at 16.

88 Webcast: Breach Notification Rule: Quarles & Brady, LLP (on file with author).

associate.[89] The security rule includes the following requirements: (1) implement security policies and procedures to safeguard ePHI; (2) conduct a risk analysis; (3) assign a security officer; (4) train workforce members; (5) sanction workforce members for violations; (6) enter business associate agreements; and (7) maintain documentation for six years.[90]

Conclusion

As we have seen in the preceding analysis and discussion, the design of the Internet was focused on resiliency, redundancy, and speed while relying on physical access security. However, as the Internet evolved and moved from a few hundred devices connected at static endpoints to a vast array of Internet-connected devices which number in the billions the need for security has become painfully apparent. From lone wolf to coordinated state-sponsored attacks, hacking efforts have increased in both frequency as well as sophistication. Consequently, it has become increasingly important to properly assess the vulnerabilities and threat factors so that reasonable steps can be taken to safeguard PII and ePHI. The IoT is transforming our lives and connecting us in ways previously unimagined. As such it is imperative that we exercise due diligence and reasonable care in order to help individuals, businesses, as well as public sector entities, become "lawsuit-proof." Just as businesses have a duty to care for their customer's data, so too, does the lawyer have a duty to ensure that client data is protected in a reasonable manner. Law Firms and lawyers simply cannot afford to be the weakest-link in the cybersecurity chain and a failure to address cybersecurity could place a firm's viability in serious jeopardy.

89 *Id.*

90 *Id.*

Constitutional Issues Raised by the Development of Microbial Cloud Analysis

Daniel M. Hart[1]

Abstract

Microbial analysis is a developing technology that could possess evidentiary value equal or greater than DNA analysis, and thus could be regulated in similar ways. The use of comparable techniques, using human DNA acquired under lessened burdens, have been limited to identification by Supreme Court and Circuit Court decisions so that they do not violate 4th amendment protections. The key difference is that microbial cloud analysis does not use human DNA. Microbial cloud analysis can gather intimate information using only a few hours of microbial deposits. This information can be used to make identifications, but can also be used to infer physical characteristics and personal habits that otherwise would not come to light. This note will consider the use of currently available microbial cloud analysis and how courts deal with DNA evidence used for comparable ends in an attempt to predict what implementations of microbial cloud analysis might be allowed by the courts of the future.

As scientific knowledge accumulates we gain a greater understanding of our bodies, our environment, and the interaction between them. The ever increasing understanding of what governs human health has led to new medicines, treatments, and

1 Syracuse University College of Law, Juris Doctor Candidate 2017. Special thanks to Professor Sanjay Chhablani for his guidance from the inception of my thesis and throughout the development of this note. Special thanks to the members of the Syracuse Journal of Science and Technology, of who I am proud to number amongst, without whose hard work this note could never have reached publication.

lifestyles. This first part of this note will be dedicated to gaining a basic understanding of the field of microbial analysis and the recent advancements in microbial cloud analysis.

These same scientific advancements have also lead to a greater understanding of life and death, how to determine a cause of death, or how to cause it. The rise of global terrorism and the threat of mass attacks on civilian centers has changed what we fear in a weapon. We have devices and protocols to test for nuclear and chemical weapons. For biological weapons we are still developing appropriate countermeasures. The ability to detect and analysis microbes in the field could be vital to defending ourselves against such attacks. The threat of a biological weapon is an extreme example of when microbial cloud analysis could be useful, one out of many that will be explored in this note. Other applications are not as flashy, identifying and tracking perpetrators or proving association through shared microbes as examples, but could have equally significant impacts. The second part of this note will concern the ramifications of microbial cloud analysis.

Microbial cloud analysis' potential for information gathering is great, but so is its potential for abuse. Looking to how courts have handled other similar technologies, such as new types of DNA analysis, can inform us on how microbial analysis might be restrained. The line between aiding law enforcement and protecting civil liberties is as fine as ever. The third and final part of this note will deal with possible legal restrictions on microbial cloud analysis' use.

I. *The Science*

In order to understand how microbial cloud analysis might change how we collect evidence and define constitutional limits we must first have a basic understanding of what the human microbiome is. Human beings host a diverse range of microbes, many of which are unique to the human body.[2] It is estimated that an average human body

2 James F. Meadow et al., *Humans Differ in Their Personal Microbial Cloud*, PeerJ, 1 (Sept. 22, 2015), https://peerj.com/articles/1258/.

contains ten foreign microbial cells for every human cell.[3] These microbes are deposited by a human body through direct contact with an environment's surface, through the shedding of skin cells and hair follicles, and through the exhalation of breath.[4] The active shedding and exhalation of microbes form what we call the microbial cloud, a halo of microbial activity emitted from our bodies, which remains suspended for a time before it settles to the ground. The average human sheds 10^6 particles per hour, many of which contain living bacteria.[5]

Usually when one considers foreign cells within the human body, they are concerned with harmful invaders rather than helpful long-term residents. We never notice the symbiotic microbes as their presence ensures our good health, if anything we would notice their absence. Though an individual's microbiome is not truly part of their body, it is personalized to the point where it may be useful to think of it as such for the purpose of conceptualizing how it may be used.

Non-pathogenic microbes now receive increased attention due to the discovery of their integral roles in healthy human functions, their presence indicating an average human body rather than one suffering from disease.[6] The effect of human released bio-aerosols, airborne biological particles that can include bacteria, on a built environment microbiome has not been the focus of study in the past.[7] This is because it is difficult to differentiate between microbes that were released from the human body and remained suspended and those that settled to a surface and were re-suspended after being disturbed.[8]

---

3 Jonathan Eisen, *Meet your Microbes*, TED TALK (Apr., 2012) 2:50-3:10, http://www.ted.com/talks/jonathan_eisen_meet_your_microbes#t-152626.

4 Meadow et al., *supra* note 2, at 1-2.

5 *Id.* at 2.

6 Meadow et al., *supra* note 2, at 2.

7 *Id.*

8 *Id.*

A continuously suspended microbial cloud may contain microbes that do not survive the settling and re-suspension process, and thus would remain undetected through other means.[9] As recently emitted microbes are more likely to be alive, there is a greater chance of them re-colonizing new humans they encounter.[10] Studying the emitted cloud could offer greater insight into how humans' microbial clouds change in response to each other's presence.[11]

A. *A Specific Advancement in Microbial Cloud Research, "Humans differ in their personal microbial cloud"*

Researchers from the University of Oregon and associated research institutions, led by James Meadow, embarked on a study to determine what they could discover by analyzing a freshly shed microbial cloud.[12] The team created a highly controlled environment to analyze the microbes that were shed and remained suspended.[13] A custom Climate Chamber at the Energy Studies in Buildings Laboratory in Portland, OR, was lined with cleanroom plastic sheeting and sealed with cleanroom tape.[14] The Chamber supplied filtered air through a ceiling plenum, which was exhausted through a floor plenum.[15] The plastic sheeting and room division was not necessary for the purposes of the second experiment; the Chamber alone sufficed.[16]

i. *The First Experiment*

Three individuals were placed in the specially divided Climate Chamber that was sterilized and equipped with air filters, to collect the suspended microbial cloud, and

9 *Id.*

10 *Id.* at 3.

11 Meadow et al., *supra* note 2, at 3.

12 *Id.* at 1.

13 *Id.* at 3.

14 *Id.*

15 *Id.*

16 Meadow et al., *supra* note 2, at 3.

petri dishes, to collect the settled microbial shedding.[17] Each subject was kept within its chamber for a two-hour and a four-hour period.[18] At the end of these periods the air filters were compared to the petri dishes as collective methods, and the results as a whole were compared to samples taken from structurally identical, but unoccupied, chambers.[19]

Sequencing the DNA of the microbial deposits collected in the filters and the petri dishes revealed that a human presence could be detected solely from the filtered air samples.[20] Testing for human specific microbes, those that live within human beings and would not appear without a human presence, accurately separated the occupied and unoccupied chambers.[21] The samples taken from the air filters revealed a human presence at both the two and four-hour intervals for all three test subjects, while the petri dishes returned the same results for two of them, only revealing the third participant after four hours.[22]

The usefulness of this technology might seem underwhelming, the value of distinguishing between occupied and unoccupied spaces being low under ordinary circumstances. However, the first experiment revealed results that prompted a second experiment, as the individuals could be distinguished from each other by the differences in the microbes they shed.[23] Each of the first experiment's three subjects released different amounts of bacterial and viral microbes at different rates.[24] Among the bacteria tested for, each subject carried unique strains and varieties, and in concentrations differing

17 *Id.*

18 *Id.*

19 *Id.*

20 *Id.*

21 Meadow et al., *supra* note 2, at 9.

22 *Id.*

23 *Id.* at 3.

24 *Id.* at 11.

from their peers'.[25] The researchers had only hoped for such promising results and had to design a second experiment to pursue this new avenue of study.

ii. *The Second Experiment*

The second experiment tested eight individuals for only ninety minutes each.[26] Twelve bacterial families were chosen as targets of the second experiment's DNA testing as they were reliable indicators of human generated microbial clouds and were indicative of a healthy human body.[27] These bacterial families are known as operational taxonomic units (OTUs) for the purposes of indicator analysis.[28] These particular bacterial families are comprised of strains of bacteria that are so closely related as not to warrant different names, but are still measurably distinct.[29]

Each of the eight subjects' presence could be detected, but whether they could be distinguished as individuals depended on the rate they shed their microbial cloud and what percentage of their shed microbes were within the twelve bacterial OTUs tested for.[30] If an individual's microbial cloud sample was comprised of the targeted bacteria by at least 20% it could be used to identify them.[31] Samples that fell below 20% could not be matched to a subject.[32]

Though the researchers were only attempting to discern the identities of the subjects, their results managed to reveal some cursory personal information. One of the subjects was strongly associated with a Lactobacillus OTU, which in their case was

---

25 *Id.*

26 Meadow et al., *supra* note 2, at 3.

27 *Id.* at 11.

28 *Id.* at 9.

29 *Id.*

30 *Id.* at 12.

31 Meadow et al., *supra* note 2, at 12.

32 *Id.*

a 100% genetic match for the Lactobacillus crispatus bacterium.[33] The significance of this association is that the Lactobacillus crispatus bacterium is commonly found dominating healthy vaginal samples; its detection correctly identified the only physically female subject of the study.[34] Physical sex is basic information that can usually be discerned through observation, but in a situation with no witnesses, it could serve as a vital first step in making an identification. The range of bacteria tested for was intentionally limited, future testing may be able to cover a wider range and identify individuals with greater accuracy.

The eight subjects of the second experiment all possessed the common human specific bacteria, but distinguishable strains of those bacteria in different proportions.[35] As identifiability will most likely rely on the most common human inhabiting bacteria, the subtle variations within species and strains level will become the markers that microbial cloud study relies on to prove its worth.[36] The identifications by microbial cloud most likely depended on the sterilized state of the collection chambers and that the clouds were sampled without the chance of commingling with another person's shedding.[37] It would be difficult to sample an individual's specific microbial signature from a crowded room with mixing clouds, but if the signature was already recorded, it might be possible to identify it among the many.

B. *Advancements in the Field of Microbial Analysis as a Whole*

The analysis of the microbial cloud is only a branch of the study of microbiomes. Developments in the parent field will have a direct impact on how quickly microbial cloud analysis develops and how effectively it can be implemented in real life situations.

---

33 *Id.* at 11.

34 *Id.*

35 *Id.* at 12.

36 Meadow et al., *supra* note 2, at 12.

37 *Id.* at 17.

The study of microbiomes is vast and varied, once microbial cloud analysis is perfected it will offer different advantages to each subdivision of the field.

i. *Calls for the Creation of a National Database*

Leading scientists within the field of microbiology have petitioned the United States government to lead an initiative to better understand the microbial communities vital to natural systems, both ecosystems and human systems.[38] The microbiologist community extends far past forensics or even health concerns, every natural environment, from undersea volcanoes to arid deserts, has a microbiome that must be understood to understand the whole.[39]

On the macro scale the Gulf of Mexico's microbiomes were altered by the Deepwater Horizon oil spill.[40] As ocean microbes are responsible for producing half of the world's oxygen, any effect on them will have repercussions for every human.[41] Better understanding of microbiomes could lead to new climate change prevention or ways to increase crop production. On the micro scale, an intestinal infection can destroy helpful gut microbes and leave an individual unable to properly digest food and absorb nutrients.[42] Simple transplantations of microbial communities have been successful, intentionally infecting a human who had lost their own microbiome with that of a close relative, but manipulating individual microbes for select health concerns is much more complicated, and has yet to be achieved.[43]

A national database to collect and exchange information could be vital to

---

38 Carl Zimmer, *Scientists Urge National Initiative on Microbiomes*, The New York Times (Oct. 28, 2015), http://www.nytimes.com/2015/10/29/science/national-initiative-microbes-and-microbiomes.html?_r=3.

39 *See id.*

40 *Id.*

41 *Id.*

42 Zimmer, *supra* note 38.

43 *Id.*

tackling such concerns, as well as making the forensic application more feasible. An international database might even be possible. Researchers in China and Germany have joined in the call for such a database.[44] In February of 2015 the National Science and Technology Council (NSTC) established a Fast Track Action Committee on Mapping the Microbiome (FTAC-MM) to explore what federal investments would be required to enable a predictive understanding of Earth's microbiomes.[45]

The FTAC-MM examined federal spending for the last three years of microbiome research and interviewed the federal researchers and program managers as to what difficulties they faced.[46] The FTAC-MM report, released November 20, 2015, revealed that the National Institute of Health received the majority of the federal funding, focusing on understanding the human microbiome.[47] The difficulties the federal researchers faced were all linked to the relative youth of the field of study; the needs "for software to analyze the large quantities of data being produced by current studies" and "to recruit bioinformaticians with the necessary computation and modeling skills to interpret the results."[48] The researcher also lamented "the lack of standards for different components from microbiome research and the need for reference materials, baseline data, and sample repositories of microbiomes and individual organisms."[49]

The FTAC-MM's report indicated the keys to microbiome research are interdisciplinary cooperation, development of set standards and references, and the creation of

---

44 *Id.*

45 Elizabeth Stulberg & Jo Handelsman, *Mapping the Earth's Microbiomes*, THE WHITE HOUSE (Nov. 20, 2015, 4:14 PM), https://www.whitehouse.gov/blog/2015/11/20/mapping-earths-microbiomes.

46 *Id.*

47 *Id.*

48 *Id.*

49 *Id.*

a user-friendly, adaptable, database for researchers to access and contribute towards.[50] The White House Office of Science and Technology Policy (OSTP) issued a national call to all microbiome researchers, asking them to share with them the details of their current research or organizational efforts.[51] The OSTP is especially interested in new interdisciplinary programs and platform technologies, such as reference libraries and databases, which could better facilitate advances in the field as a whole.[52]

The OSTP may use the response to direct federal funding in the future, or organize collaborations between parties that otherwise would never come into contact. The interest of the federal government makes the prospect of national microbial database much more realistic and the idea of using microbial evidence in everyday forensics work all that more feasible.

ii. *"Home Grown" Bioterrorism*

When bioterrorism is considered one of the first examples to come to mind is the use of anthrax laden envelopes, coming into the public eye in the early 2000s.[53] These envelopes took at least five lives, the rarity of the disease and wide range of the attacks complicating the response.[54] These envelopes were considered extremely dangerous, prompting several studies on their effects.[55]

Countering a biological attack would require the work of multiple disciplines,

---

50 *Id.*

51 Jo Handelsman & Elizabeth Stulberg, *Calling All Microbiome-Science Champions!*, The White House (Jan. 27, 2016, 10:27 AM), https://www.whitehouse.gov/blog/2016/01/27/calling-all-microbiome-science-champions.

52 *See id.*

53 Paul Keim, *Microbial Forensics: A Scientific Assessment*, American Academy of Microbiology, 5.

54 Keim, *supra* note 53, at 8.

55 Igor E. Agranovski et al., *Bioaerosol Contamination of Ambient Air as the Result of Opening Envelopes Containing Microbial Materials*, 39 Aerosol Sci. and Tech.,1048, 1048 (2005), *available at* http://dx.doi.org/10.1080/02786820500380230.

depending on how the attack is delivered.[56] The attack might make use of a natural or engineered pathogen, be aimed the population or food and water sources, and require physical analysis or genomic sequencing.[57] It could be designed to have delayed effects, making it more difficult to track to its source and the perpetrator.[58] The customizable nature of biological weapons make them difficult to plan for. That these weapons could potentially be created from mundane materials, such as common bacteria altered to produce uncommon effect, makes them difficult to regulate.

The great variety requires quick and efficient cooperation between specialists, which could only be achieved with a standardized system.[59] The proposed national database for the study of microbiomes and the exchange of research would be vital to preparing the nation for a biological attack. The ability to collect microbes from the air and analyze them will be essential to dealing with biological threats. Microbial cloud analysis might be able to detect pathogens before their symptoms begin to manifest and get a head start on tracking the microbes to their source. Microbial sampling could become a standard security check, like metal detectors, once the process is streamlined and analysis speed increased.

iii. *The Microbial Fingerprint*

The analysis of settled microbes is considerably more advanced than cloud analysis, having already produced some promising results. Samples of bacterial communities transferred directly from skin contact have been used to identify an individual weeks after they had been left, a feat achieved by a research team lead by Noah Fierer in 2010.[60]

---

56 Keim, *supra* note 53, at 5.

57 *Id.*

58 Duraipandian Thavaselvam and Rajagopalan Vijayaraghavan, *Biological warfare agents*, 2(3) J. Pharm Bioallied Sci., (Sept. 3, 2010), http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3148622/.

59 Keim, *supra* note 53, at 5-6.

60 Edwin Steussy et al., *Microbial Forensics: The Biggest Thing Since DNA*?, Social Science Research Network, 34 (Feb. 3, 2015), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2560109.

A microbial deposit left through direct contact is known as a "microbial fingerprint." Bacterial communities left on keyboards and computer mice, left at room temperature for several weeks, were easily associated with their sources out of 270 control samples.[61]

More difficult than matching a fresh sample to a dead one is matching two living samples; tracking a microbe after it was shed and re-colonized a second human being. Both pools of microbes continue to evolve into unique strains, becoming more distinct as time passes.[62] An evolutionary analysis of shared genes can locate a common ancestor, if there is one, and estimate how long ago they broke away.[63] This could be used to determine if two people had been in contact with each other, closely and regularly so that microbial re-colonization would be expected, and how long ago that contact was. Studies have shown that skin bacteria is shared between family members and other cohabitants, including family pets.[64] The result of cohabitation is that their bacterial communities are far more similar to each other's than they are to those outside the home, though nowhere close to being identical.[65]

iv. *The Home's Microbiome*

Jack Gilbert leads the Home Microbiome Study with the purpose of collecting microbial samples to better understand how environmental factors shape microbial community structures.[66] The study followed seven U.S. families over six weeks by regularly sampling their skin and home surface bacterial communities.[67] The study con-

61 Steussy et al., *supra* note 60, at 33-34.

62 *Id.* at 13-14.

63 *Id.* at 14.

64 *Id.* at 34.

65 *Id.* at 34.

66 *About*, Home Microbiome Study (last accessed Jan. 1, 2016), http://homemicrobiome.com/about/.

67 Jack A. Gilbert et al., *Longitudinal analysis of microbial interaction between humans and the indoor environment*, Science (Aug. 29, 2014), http://www.sciencemag.org/content/345/6200/1048.full.

firmed that cohabitants shared similar bacterial skin communities, most so in the bacteria dwelling on their hands.[68]

Three of the families moved mid-study, but comparisons of the bacterial communities of their old homes and their new ones revealed only slight discrepancies, suggesting the families' microbial signatures rapidly colonized the new spaces.[69] This rapid colonization by a foreign microbial community could potentially grant insight to a confusing order of events. If the microbial community of a living space does not match those who supposedly dwell there, it could prove that other parties had been intruding for an extended period of time

II. *Potential Ramifications of Microbial Analysis*

The microbial cloud study has generated increased attention for the growing field of microbial analysis. Interest in the forensic applications of microbial cloud analysis has stirred, but it is thought that the techniques require considerable improvement before the results can be considered reliable.[70] The potential of microbial analysis has caught more than just the public's attention. The Department of Justice's (DOJ) Office of Justice Programs awarded a grant to the University of California, San Diego (UCSD) to research the potential forensic applications of analyzing microbes left by touch.[71] The "microbial fingerprint" of a human, which is the trace of bacteria and fungi left after touching an object, is less ephemeral than the microbial cloud and does not require a closed space.[72] The DOJ has given $637,942 to UCSD to investigate the uses and lim-

68 *Id.*

69 *Id.*

70 Jeffrey Kluger, *Congratulations, You Have Your Own Personal Germ Cloud*, TIME (Sept. 23, 2015), http://time.com/4044393/microbe-cloud-microbiome/.

71 Brie Stimson, *Researchers To Test Feasibility of Microbial Cells as Crime Scene Evidence*, NBC SAN DIEGO (Sept. 20, 2015), http://www.nbcsandiego.com/news/local/Researchers-To-Test-Feasibility-of-Microbial-Cells-as-Crime-Scene-Evidence--328455771.html#ixzz3vpGX5Zyy.

72 *Id.*

itations of the "microbial fingerprint".[73]

Analysis of settled microbial communities, those no longer airborne, is more developed than purely airborne or freshly settled analysis, but can be instructive on how airborne data could be used. Preparations for the increased introduction of microbial evidence in court have already begun, focused in criminal forensics.[74] *Microbial Forensics: The Biggest Thing Since DNA*?, which was co-written by attorneys and scientists, was published in the UC Davis Legal Studies Research Paper Series for the express purpose of familiarizing the criminal law community with the core concepts of microbial forensics.[75] One of the case studies within this paper perfectly illustrates the application of microbial forensics and is summarized later on.

A. Effects of a Microbial Community's Mutability

The DNA profile of a human's microbial community, unlike a human's DNA, is not fixed. Bacteria can reproduce in as little as fifteen minutes and viruses within a day, with every new generation there is the possibility of mutation and genetic drift from a common ancestor.[76]

This genetic drift is mapped using phylogenetic analysis, "the study of evolutionary relationships between groups of organisms."[77] Phylogenetic analysis allowed biologists to create what is commonly known as evolutionary trees or trees of life. Trees of life are visual representations of how long ago modern species diverged from other known species. Evolution works much faster in microbes than in animals, which means

---

73 Dep't of Justice, *Detailed information for award 2014-R2-CX-K411*, Office of Justice Programs, https://external.ojp.usdoj.gov/selector/awardDetail?awardNumber=2014-R2-CX-K411&fiscalYear=2015&applicationNumber=2015-90189-CA-DN&programOffice=NIJ&po=All, (last visited Mar. 12, 2016).

74 Steussy et al., *supra* note 60, at 5.

75 *Id.*

76 *Id.* at 12.

77 *Id.* at 13.

microbes shed hours earlier and a fresh sample may not be genetically identical, but will likely be close enough to draw inferences and make a match.[78] Tracking the differences between the samples might also allow an estimation of how much time has passed since the deposition.

B. *Potential Consequences of the Home's Microbiome*

Jack Gilbert's study of a home's microbiome did not take air samples or test the air filters as they were more focused on tracking microbes left through touch and those living on related surfaces. These sources can be useful, but cannot offer a complete picture. The microbes living on the surfaces match the occupants of that space and would not reflect short-term visitors. The "microbial fingerprint" is left when a human touches a surface, the same surfaces where DNA evidence or actual fingerprints would be left and subsequently would be the first surfaces to be sterilized in an attempt to destroy evidence.

Evidence left through physical contact would not be foolproof in dealing with a home invasion situation, assuming the perpetrator was a stranger and knew to be careful about leaving traces behind. What they would not be able to easily, or quietly, access would be air ducts and air filters. Taking samples from the filters and using the family's microbial communities as a comparison, through process of elimination, the perpetrator's microbial profile might be composed.

C. *Field Testing in Early Stages*

Gathering and analyzing microbial deposits has become increasingly easy in recent years. The procedures necessary for collecting and properly preserving microbial samples are not that different from those required for DNA or other types of physical evidence and scientific advances have made sequencing bacterial evidence quick, accu-

78 *Id.* at 12.

rate, and affordable.[79] It used to be that microbes had to be isolated and grown in a lab after collection before they could be sequenced.[80] Many microbial species resisted the culturing process and remained hidden from human discovery until genetic sequencing became a viable alternative.[81] The advancements in microbial analysis have opened the doors for testing in field conditions.

Researchers at the Argonne National Laboratory, led by research coordinator Jarrad Hampton-Marcell and assisted by the Fort Lauderdale police department, staged a typical breaking and entering in order to test what microbial evidence they could collect and how useful it would be in identifying the burglars.[82] The "burglars" were two police officers, so their identities were known factors, but the house was a regularly occupied home that, with the homeowner's permission, was used to create realistic field conditions.[83]

In a real home, far from a sterilized lab with precisely controlled conditions, the challenge was to gather microbes from the burglars while differentiating them from the homeowners and their cat.[84] Not only was Hampton-Marcell and the Argonne National Laboratory team able to distinguish between the "burglars" and the lawful residents, they uncovered personal medical information about their subjects through their microbes.[85]

The bacteria collected and matched to the "burglars" indicated two specific

---

79 *See* Mandy Oaklander, *A Strange New Way to Solve Crimes*, TIME, Aug. 31, 2015, at 44, 46.

80 *Id.* at 47.

81 Steussy et al., *supra* note 60, at 9.

82 Oaklander, *supra* note 79, at 46.

83 *Id.*

84 *Id.*

85 *Id.* at 47.

conditions, regular drinking and migraines.[86] The bacteria matched to the homeowners indicated an omnivorous diet and a dedication to vitamin B and calcium supplements.[87] One of the officers does get migraines and the homeowners do have balanced diets supplemented with vitamins.[88] Whether one of the officers is a regular drinker was either not explored or not recorded, for obvious reasons. It's those reasons, the risk of personal information falling into the wrong hands, which raises ethical questions as how to properly regulate microbial analysis when it becomes common in the field. The personal information gained from microbial cloud analysis would surely benefit law enforcement, but the ease of collection seems inappropriate when compared to the value of the insight.

D. *Specific Advantages of Microbial Analysis*

Human microbiome analysis has risks in that the source is unfixed, but the advantage is that the microbial community changes depending on the actions of the host and the company they keep. Rather than representing a biological identity, as human DNA does, microbial DNA reflects an individual's life occurrences. Microbial deposits might reveal that its former host was a vegetarian, or a drug user, or owned a dog, or any number of little details that could shrink a suspect pool.

Forensic research laboratories are currently developing techniques to exploit the microbial cloud. Common goals include, but are not limited to, increasing the accuracy in estimating time of death, obtaining personal identification based on skin microbial communities, identifying types of body fluid residue, and tracking a soil sample back to its source.[89] While an individual's bacterial community can change over time, the extent to which it can change is typically much less than the difference between individuals;

86 *Id.*

87 Oaklander, *supra* note 79, at 47.

88 *Id.*

89 Steussy et al., *supra* note 60, at 26.

this relative stability preserves its uniqueness and makes it a reliable source of identification.[90]

Proving relationships between people based on their microbiomes has already been established in courts of law, though the focus has been on dangerous pathogens and the legal ramifications of spreading those pathogens. Tracking infection from a single source to a large group of victims requires proving the strain is related and that the source has carried the infection for the greatest amount of time.

The team behind *Microbial Forensics: The Biggest Thing Since DNA?* chose to focus on a foreign case to showcase how microbial analysis can be implemented within the courtroom, an example which is heavily relied on here to establish groundwork.[91] The Spanish prosecution of Dr. Juan Maeso for the infection of his patients with Hepatitis C relied on phylogenetic analysis and the "molecular clock."[92] The Spanish court asked academic geneticists from Valencia to prove a connection between Dr. Maeso and the outbreak group.[93] A phylogenetic analysis of Dr. Maeso's Hepatitis C virus (HCV) and of those in the potential outbreak group proved they were closely related, in comparison with those in a control group.[94] After proving the relationship, the court-appointed experts had to prove that it was the doctor that infected his patients, rather than an unknown third party or source.[95]

A molecular clock is a formula through which an approximate date of infection can be calculated. Viral mutation rates are relatively standard, though there are different

90 *Id.* at 33.

91 *Id.* at 15.

92 *Id.* at 20-21.

93 *Id.* at 17.

94 Steussy et al., *supra* note 60, at 19.

95 *Id.* at 20.

rates for different species and subspecies.[96] If an investigator knows the infection date and number of mutations, they can calculate the mutation rate.[97] Dr. Maseo's case, twenty-four patients who had only a single contact with the doctor tested negative for HCV before their surgeries, but tested positive afterwards.[98] With this data the scientists were able to create a time formula and map the likely infection dates for each patient.[99] The molecular clock established that many of the prospective victims' infections dates did not contradict the court's hypothesis of infection during surgery, and the greater number of mutations in Dr. Maseo's virus suggested he was the first of them to be infected and the most likely source.[100]

While Dr. Maseo's case involved a harmful pathogen, there is no reason why the same techniques could not be applied to more mundane microbes. Hepatitis is much easier to contract than other microbes and is rarer than those commonly found in every human, making it suitable to be tracked along routes of infection. Pathogens like it are also likely to be at the forefront of whatever legal matters microbial analysis would be implemented in, due to their detrimental effects. These techniques would be essential to countering intentional infections, such as biological warfare, in order to find the source and eliminate the threat. It is the more mundane applications that will have a greater impact on the average person's life.

If it is not the infection that is important, but rather the association that caused the infection, non-pathogenic microbes are just as useful. It is easy to think of a situation in which one party want to prove another party was sleeping with a third, not for the purposes of dealing with a dangerous sexually transmitted infection, but to use that

---

96 *Id.*

97 *Id.*

98 *Id.*

99 Steussy et al., *supra* note 60, at 20.

100 *Id.* at 20-21.

information in civil litigation. If microbial analysis can prove a spouse and third party share microbes that would only be likely to repopulate in close quarters and over time, the other spouse would want to bring that into divorce proceeding or perhaps a child custody battle. By itself it is not proof of an affair, but would be suggestive.

Proving conspiracy might also benefit from microbial analysis. Microbial signatures are almost entirely set, but do change in response to new people and environments. Microbial analysis could be used to supply evidence that a group of people had been meeting together, or at least all frequented the same location, even if they claimed to have no connection to one another. Just as the group would begin to resemble each other, their meeting place would develop a microbiome based on all of their settled microbial clouds. That a microbiome changes through experience is not a weakness or a sign of unreliability, simply a new feature of personal identity waiting to be fully exploited in the pursuit of evidence.

III. *Potential Future Restrictions Based On Similar Existing Technologies*

Microbial cloud analysis is not developed to the point where it can be employed to gather evidence, but it shows promise. There currently exists no nationwide database by which to compare samples taken or standardized method of collection from crime scenes or suspects. The methods of analysis have not been tested under harsh enough conditions that their reliability could be counted on. While the implication of microbial cloud analysis could improve national defense, applications to the average citizen should be considered with caution. Working under the assumption that these methods will be perfected, they will most likely meet the same privacy concerns that DNA evidence is currently faced with.

A. *Touch DNA*

The term touch DNA refers to DNA that is left behind after a person touches or

otherwise comes into direct contact with a physical item.[101] Touch DNA is not visible to the naked eye and is gathered by identifying items that would likely be touched, and are the type of material to hold onto the cells over time, then properly collecting and storing these items as to preserve those traces.[102]

Touch DNA came to public prominence when it was instrumental in clearing the family of JonBenet Ramsey of all suspicion in her unsolved murder.[103] JonBenet Ramsey was a six year old child-beauty pageant contestant who was found strangled in the basement of her home in 1996, the circumstances of her death invoking a period of media sensationalism.[104] None of her family members were ever charged with her murder, but they continued to live under a cloud of suspicion as no other suspects had been identified. They suffered under this stigma until 2008, when touch DNA left on JonBenet Ramsey's clothing proved the involvement of an unrelated and unidentified male.[105]

In *Raynor v. State*, Glenn Raynor was given a 100-year sentence for committing a heinously violent rape when DNA he left on the arms of a chair was matched to that left at the crime scene.[106] Raynor was interviewed by the police in connection to the unsolved rape, voluntarily coming to the station when requested, but perspired heavily under the pressure and excused himself.[107] The sweat left on the chair arms contained

---

101 Angela L. Williamson, *Touch DNA: Forensic Collection and Application to Investigations*, J Ass'N Crime Scene Reconstruction, Sept. 18, 2012, at 1, http://www.acsr.org/wp-content/uploads/2012/01/Williamson.pdf.

102 *Id.*

103 *DNA Clears JonBenet's Family, Points to Mystery Killer*, CNN (July 10, 2008), http://www.cnn.com/2008/CRIME/07/09/jonbenet.dna/.

104 *Id.*

105 *Id.*

106 *Law Professor Asks Supreme Court to Hear DNA Case*, University of Baltimore (Feb. 3, 2015), http://www.ubalt.edu/news/news-releases.cfm?id=2165.

107 *Id.*

enough viable DNA to make a match.[108] Raynor appealed the conviction claiming that collecting the sweat was an unlawful search and violated his 4th amendment rights.[109] The Court of Appeals of Maryland confirmed the lower court's ruling, that the analysis of 13 specific noncoding portions in the genetic code could only be used for identification purposes, and as there was no danger of personal genetic information being misused by authorities there was no violation of his fourth amendment right to privacy.[110] The Supreme Court has refused to hear his case on appeal, effectively supporting the lower court's reasoning through its silence.[111]

Touch DNA has been limited to identification; no personal information that might be a source of prejudice or be misused during interrogations can be gleaned from it. The 13 loci analyzed in touch DNA were chosen because they are highly variable between individuals and do not include specific information such as sex, race, personal health or genetic disease.[112] It is with the reassurance that this DNA will be used solely for identification purposes, and not used to create a genetic profile to search for a perpetrator or take advantage of a genetic disease during a high-pressure interrogation, that courts have allowed its collection and use without warrants.

The same concerns that limit the use of touch DNA will inevitably arise when microbial analysis enters the courts. Analysis of microbiome can reveal details about physical sex, health, habits, and numerous other aspects of an individual's life that could be considered a serious invasion of their personal privacy. If we consider the micro-

---

108 *Id.*

109 Raynor v. State, 99 A.3d 753 (Md. 2014), *reconsideration denied* (Oct. 21, 2014), *cert. denied*, 135 S. Ct. 1509 (2015).

110 *Id.* at 763.

111 Lydia Ramsey, *Your DNA can now be Used Against you in Court Without Your Consent*, Popular Science (Mar. 3, 2015), http://www.popsci.com/supreme-court-just-effectively-made-it-possible-your-dna-be-used-against-you-criminal-court-without.

112 Max Houck & Lucy Houck, *What is Touch DNA?*, Scientific American (Aug. 8, 2008), http://www.scientificamerican.com/article/experts-touch-dna-jonbenet-ramsey/.

biome to be part of a body and an extension of that person it might warrant the same protections extended to genetic code. Sound arguments can be made against this view; the microbiome is not fixed to identity the same way DNA is, it can change over time and under certain circumstances be completely erased or replaced. It is also developed in part by personal actions, within an individual's control.

B. *Increased Ease of DNA Collection*

Concerns over how DNA is used also arise\ over how it is collected. Touch DNA is only allowed without a warrant if it only used for identification, and only because it does not involve any violation of the body itself. State statutes have been passed allowing DNA to be collected after arrest or minimal suspicion, upheld by Federal Circuit Courts, holding that they do not violate the fourth amendment due to how they are implemented.

California's Proposition 69 allows for the taking and retention of DNA samples of anyone arrested on the suspicion of committing a felony; it was immediately challenged as a violation of the right to be free of unreasonable searches and seizures.[113] While the Ninth Circuit Court was debating the constitutionality of the act, the Supreme Court found a very similar DNA collection program in Maryland to be constitutional.[114] The Maryland program allowed inner cheek swabs to be taken without the arrestee's consent.[115] Based on the Supreme Court decision, the Ninth Circuit Court of Appeals upheld the more expansive Californian DNA collection program to be constitutional.[116]

A similar program was evaluated in the Third Circuit. The DNA Analysis

113 Maura Dolan, *Federal Appeals Court to Reconsider California DNA-Collection Law*, Los Angeles Times (July 26, 2012), http://articles.latimes.com/2012/jul/26/local/la-me-dna-court-20120726.

114 Maryland v. King, 133 S. Ct. 1958 (2013).

115 *Id.*

116 Haskell v. Harris, 745 F.3d 1269, 1271 (9th Cir. 2014).

Backlog Elimination Act, permitted the suspicionless collection of DNA samples from arrestees and pretrial detainees. [117] The Act has Fourth Amendment protection built in, limiting the analysis to "junk DNA", the highly variable non-coding stretches of DNA, and the purpose to identification.[118] A petition to the 3rd Circuit Court of Appeals has been denied.[119]

DNA collection programs with low requirements for searches have the same limitations as those applied to touch DNA. They are both limited to analyzing coding that does not reveal personal information and restricting the use to identification, because they both threaten to put inappropriate amounts of citizens' personal information into the hands of the authorities. As microbial analysis raises similar concerns it is reasonable to expect it will bear similar restrictions. This is assuming that policy concerns are guiding how the evidence is managed, rather than the source of the evidence itself.

C. *Mitochondrial DNA*

Mitochondrial DNA is another source of genetic identification that has recently become accepted to use in the American court system. Mitochondrial DNA differs from touch DNA in that it is not the collection method that is atypical, but the DNA itself. Mitochondrial DNA is not what most think of as DNA, the double helix existing in the center of the cell (nuclear DNA). Rather, mitochondrial DNA is drawn from human mitochondria, organelles that exist within the human cell but outside the cellular nucleus.[120]

Human cells can contain hundreds of copies of mitochondrial DNA, in stark contrast to the two copies of nuclear DNA, greatly increasing the likelihood of obtaining

117 United States v. Mitchell, 652 F.3d 387, 404 (3d Cir. 2011).

118 *Mitchell*, 652 F.3d at 402.

119 Mitchell v. United States, 132 S. Ct. 1741, 182 L. Ed. 2d 558 (2012).

120 *Forensic DNA: Mitochondrial DNA*, National Institute of Justice, http://www.nij.gov/topics/forensics/evidence/dna/research/Pages/mitochondrial.aspx?tags=Mitochondrial%20DNA (last modified Dec. 23, 2013).

a viable sample.[121] This becomes vital when the source of the DNA is extremely small or the DNA has become damaged or degraded in some way.[122] Mitochondrial DNA has allowed forensic investigations in situations where biological samples are limited, such as missing persons cases in which the main source cannot be found, or mass disasters in which bodies may be left in pieces or intermingled and exposed to the elements.[123]

Mitochondrial DNA is easier to recover than regular DNA and follows a unique pattern of inheritance. Mitochondrial DNA is maternally inherited and undergoes no recombination or alteration.[124] Unless a mutation occurs, any individual will have identical mitochondrial DNA to his or her mother, siblings and maternal half-siblings, and all maternal relatives.[125] Forensic comparisons can be made by using a sample from any maternal relative, even if the relative and the subject are separated by countless generations.[126]

In *State v. Council* mitochondrial DNA (mtDNA) was used to disprove the appellant's alternative explanation for what happened.[127] While nuclear DNA is only found in the living root of the hair, mtDNA can be harvested from the strand of hair itself.[128] The mtDNA drawn from the hairs at the scene proved that the man Council had pinned the blame on could not have committed the crime, while he himself was still a valid candidate.[129]

---

121 *Id.*

122 *Id.*

123 *Id.*

124 *Id.*

125 *Forensic DNA: Mitochondrial DNA*, *supra* note 117.

126 *Id.*

127 State v. Council, 515 S.E.2d 508, 516 (S.C. 1999).

128 *State*, 515 S.E.2d 516 n.12.

129 *Id.* at 517.

IV. *Conclusion*

DNA evidence was once on the forefront of forensic technology. Over time the ability to gather and sequence genetic information improved to the point where DNA collection became commonplace. Touch DNA has expanded where we can gather DNA evidence from, changing how we view the value of objects and materials at any crime scene. Mitochondrial DNA allowed us to draw DNA from smaller and damaged samples, and established a system of maternal relationships that can quickly narrow down a suspect pool. New DNA collection programs have arisen as confidence in the field has grown, seemingly leading us towards a future where DNA is recorded as easily as fingerprints or mugshots.

This path towards easier identification seems to be limited to just that: identification. Using solely junk DNA to make the identifications makes the collection and abuse of personal information less likely. Should microbial cloud evidence be included along this path? It can surely be used to identify people and can reveal personal information, but that information is not inherent, it is developed over time and through habits and circumstances.

An individual's microbiome reflects the body's origins and history, but also the choices that person made to bring them to where they are today. People are held accountable for their appearance, even if that appearance is one of good or ill health. If the analysis of a microbiome will only reveal information that could have been accessed in other ways, is the potential harm all that great?

Should such a powerful tool be limited to identification purposes only? Individual civil rights are always a concern, but when dealing with harmful pathogens society as a whole is endangered. Even when the fate of the nation is not at stake, solving a kidnapping or a murder might be important enough to swallow some discomfort.

Microbial analysis could offer information of greater value than DNA evidence, and microbial cloud analysis could change where and when this evidence could be gathered. Air samples in police precincts and government buildings could be regularly analyzed; perhaps it could even become part of private security systems. While the methods of dealing with DNA evidence can be informative, I would advise against applying them wholesale to microbial analysis. The microbiome provides a whole new frontier of information, for both scientific and legal investigations; the management of that frontier should be allowed to develop organically, guided by past successes, but not overly constrained.

"Follow the Money and the Laws Will Follow"[1]: State Legislative Solutions to Daily Fantasy Sports

Ashley Menard[2]

Abstract:

Daily fantasy sports, which are contests where individuals choose a number of sports professionals and earn points based on those professional's performance, have surged in popularity over the past five years. With the rise of online daily fantasy sports sites such as DraftKings and FanDuel, the daily fantasy sport market has transformed into a multi-billion dollar one. However, a surge in popularity has brought daily fantasy sports into the legal forefront. The question in the U.S. remains whether daily fantasy sites are operating legally. The answer to this question turns on whether daily fantasy sports are games of "skill" or games of "chance," the latter being illegal in the U.S. A number of state attorneys general have already determined that daily fantasy sports are games of chance, thus deeming them illegal and ceasing their operation within the individual state. However, in order to ensure continued participation in daily fantasy sports, state legislatures should take action to legalize them, while creating regulatory and consumer protection frameworks. Only in this way will state residents be able to participate in daily fantasy sports in a secure environment, while at the same time benefitting individual states.

This note will first address in Section I what daily fantasy sports are, and how they are distinguished from legal traditional fantasy sports. Additionally, this note will discuss the rapid growth of daily fantasy sports in Section II, and its impact in the U.S. Next, in Sections III and IV, this note will then discuss the legality of daily fantasy sports on both a federal and state level. In Section V, this note will then address legal solutions states should take to ensure continued operation of daily fantasy sports. Last, Section VI will address the policy considerations of adopting the recommended legislative solutions.

---

1 Darren Heitner & Toni Gemayel, *The Hyper Growth Of Daily Fantasy Sports Is Going To Change Our Culture And Our Laws*, Forbes (Sept. 16, 2015, 4:01 PM), http://www.forbes.com/sites/darrenheitner/2015/09/16/the-hyper-growth-of-daily-fantasy-sports-is-going-to-change-our-culture-and-our-laws/.

2 Syracuse University College of Law, Juris Doctor Candidate 2017.

Introduction

Daily fantasy sports ("DFS") have surged in popularity over the past five years. With the rise of online daily fantasy sports sites such as DraftKings and FanDuel, the daily fantasy sports market has transformed into a multi-billion dollar one.[3] However, in 2015, daily fantasy sports were brought to the legal forefront in the United States. Many Americans are asking the question of whether online daily fantasy sport sites, are operating illegally. The industry's rapid growth has drawn the attention of state attorney's general, state legislatures, and even the Federal Bureau of Investigation and the Department of Justice.

While it is questionable whether daily fantasy sports will pass legal muster at both the federal and state levels, there is reason to believe that the daily fantasy sports business model is in legal trouble. With recent state action and attorney general opinions, many share the opinion that daily fantasy sports are in fact illegal when applying various state laws, or in interpreting federal laws. However, state legislatures should take action to legalize daily fantasy sports, while creating regulatory and consumer protection frameworks. Only in this way will state residents be able to participate in daily fantasy sports in a secure environment, while at the same time benefitting individual states.

I. What Are Daily Fantasy Sports?

Daily fantasy sports are contests where individuals several sports professionals and earn points based on those professionals' performance.[4] Daily fantasy sports are a subset of traditional fantasy sports, which have been popular in the U.S. for a number of decades. In understanding what daily fantasy sports are, it is important to understand traditional fantasy sports.

---

3 Kristin Wong, *The Fantasy Sports Industry, by the Numbers*, NBC News (Oct. 6, 2015, 7:44 PM), http://www.nbcnews.com/business/business-news/fantasy-sports-industry-numbers-n439536.

4 *Introduction to Fantasy Sports*, Fantasy Network, http://www.fantasynetwork.com/about-fantasy-sports/.

A. *Traditional Fantasy Sports*

Traditional fantasy sports are season long contests that a group of people compete in together.[5] The most popular type of traditional fantasy sport contest is where an "owner" of a fictional team selects a roster of players in a particular sport to create a team.[6] Participants must choose players from a variety of professional teams at the beginning of the season, typically through a draft where each participant picks one professional at a time.[7] After creating a team, points will be earned throughout the season based upon the statistics that the players achieve.[8] In most professional sports, points gained in fantasy sports are for accomplishments on the field, such as a hit in baseball, yards gained in football, or a basket in basketball.[9] During the season, owners have the opportunity to trade players, cut players from his or her roster, and sign new players. [10] The goal is to accumulate more fantasy points than anyone in the league, either on a week-to-week basis or throughout the entire season.[11] Oftentimes, the winner of the league will receive a payout.

Traditional fantasy sports were created at the end of the 1950s, and began gaining popularity in the 1980s.[12] The biggest innovation in fantasy sports came with the internet, which caused established fantasy sports businesses to migrate online.[13] Today, many companies, such as Yahoo, ESPN, NFL, CBS and Fox Sports, offer their own

---

5 *Id.*

6 *Id.*

7 *Id.*

8 *Fantasy Sports Betting*, BOVADA, https://sports.bovada.lv/content/fantasy-sports.

9 *Id.*

10 *Id.*

11 *Introduction to Fantasy Sports*, *supra* note 4.

12 *Fantasy Sports Betting*, *supra* note 8.

13 *Id.*

competitions through their own online platform.[14] These sites include leagues in a long list of sports, the most popular being American football, baseball, basketball, and hockey.[15] Other sports that are offered include golf, soccer, NASCAR and rugby.[16]

B. Daily Fantasy Sports

Daily fantasy sports, on the other hand, are distinguishable from traditional fantasy sports in a variety of ways. Unlike season long traditional fantasy sports, daily fantasy sports last the span of a week, a day, or even a portion of a day.[17] Daily fantasy participants first choose to participate in contests where they are playing against other people - sometimes hundreds or thousands.[18] Each participant's drafted team is matched up against every other participant's team, and at the completion of the contest, one ranks somewhere in the contest and potentially receives a payout.[19]

After choosing a type of contest and when that contest will occur, a participant drafts his or her team.[20] While traditional fantasy sports leagues let only one player be on each team, multiple daily fantasy sports teams could have the same player.[21] A participant is given a salary cap to spend on his or her team, and each player is priced differently based upon his or her skills.[22] The goal of each participant is to assemble a winning combination of players within the given salary cap.[23] For example, when playing daily

---

14 *Id.*

15 *Id.*

16 *Id.*

17 Kyle Holmes, *An Introductory Guide to Daily Fantasy Sports*, The Huddle, (Aug. 26, 2015), https://www.thehuddle.com/2015/articles/daily-fantasy-sports-introductory-guide.php.

18 *Id.*

19 *Id.*

20 *Id.*

21 *Id.*

22 Holmes, *supra* note 17.

23 *Id.*

football, one may want to pay the high cost of $9,700 for Aaron Rogers but downgrade the running back position to a more affordable $6,400 Chris Ivory.[24]

In order to participate in daily fantasy sports, a participant must pay an "entry free" to potentially win a prize.[25] For example, a player could choose a contest with a five dollar entry fee, and the winners of the contest will get a specified amount of money. If a participant scores the most points among the group of players, he or she will instantly take home the winnings.[26]

II. Rapid Growth of Daily Fantasy Sports

Since daily fantasy sports came about between the years 2009-2012, there has been a hyper growth of popularity and participation.[27] According to the Fantasy Sports Trade Association ("FSTA"), 568 million people in the U.S. and Canada played fantasy sports as of January 2016.[28]

Participants in daily fantasy sports typically participate through DFS companies DraftKings or FanDuel, which control approximately ninety-five percent of the North American daily fantasy sports market.[29] New York based FanDuel began operation in 2009 while Seattle-based DraftKings began operation in 2012.[30] As of 2015, both companies were worth over $1 billion, and continue to grow at a rapid pace.[31] Also in

---

24 *Id.*

25 *How It Works*, FANDUEL, https://www.fanduel.com/how-it-works (last visited Sept. 16, 2016).

26 *Id.*

27 *See* Matthew Futterman & Sharon Terlep, *The Deals That Made Daily Fantasy Take Off*, WALL ST. J.: SPORTS SECTION (Oct. 16, 2015, 8:55 PM), http://www.wsj.com/articles/the-deals-that-made-daily-fantasy-take-off-1445043328.

28 *Research*, FANTASY SPORTS TRADE ASSOCIATION, http://fsta.org/research/.

29 Futterman, *supra* note 27.

30 *Id.*

31 Chris Korman, *DraftKings and FanDuel are fun, addictive, and completely unfair for most fans*, FTW!NFL (Sept. 18, 2015, 11:57 AM), http://ftw.usatoday.com/2015/09/daily-fantasy-sports-football-drafkings-fanduel-commercials.

2015, both companies spent millions of dollars in advertising, and people could not watch television or use the internet without seeing the two company's names.[32] Combined, the two companies spent $31 million on 9,000 ads during the first week of the National Football League season alone.[33]

The growth of daily fantasy sports has investors rapidly investing in daily fantasy sports companies.[34] As of September 2015, FanDuel had raised $361 million from media companies like Comcast Ventures, NBC Sports, and Time Warner Investments.[35] DraftKings had raised $375 million total from media companies as well, one notable investor being Fox Sports.[36]

Most notably, professional sports leagues have begun investing in daily fantasy sports companies as well. [37] DraftKings has received investments from Major League Baseball, Major League Soccer, the National Hockey League, and the Kraft Group, owned by Robert Kraft of the New England Patriots.[38] FanDuel sealed an exclusive partnership with the National Basketball Association in exchange for an equity stake in the company.[39] By investing in the companies, the professional sports leagues seek both profit and heightened viewership.[40] FTSA data states that daily fantasy sports players consume 40% more sports content after becoming players, and it no longer takes a prime-time game to engage viewers.[41] With the rise of daily fantasy sports, participants

32 Futterman, *supra* note 27.

33 Korman, *supra* note 31.

34 Heitner, *supra* note 1.

35 *Id.*

36 *Id.*

37 *Id.*

38 *Id.*

39 Heitner, *supra* note 1.

40 *Id.*

41 *Id.*

now have exciting new reasons to watch less exciting match-ups.[42]

However, with DraftKings and FanDuels rapid rise in popularity and the hyper growth of daily fantasy sports, the company's business models have been called into question on both a federal and state level. The question remains whether daily fantasy sites are operating legally or illegally.

III. Legality of Daily Fantasy Sports on the Federal Level

Gambling is subject to legislation at the federal level that bans it from curtain areas, limits the means and types of gambling, and otherwise regulates the activity.[43] For several years, daily fantasy sports have not been considered gambling, and have been seemingly legal in the United States on a state level.[44] However, as daily fantasy sports have rapidly gained popularity, its legality has been called into question.

A. Unlawful Internet Gambling Enforcement Act (UIGEA)

In 2006, in response to traditional law enforcement mechanisms being deemed inadequate in enforcing gambling prohibitions or regulations on the internet, the Unlawful Internet Gambling Enforcement Act (UIGEA) was passed.[45] This federal statute provided a new mechanism for enforcing gambling laws on the internet.[46] The statute provides that no person engaged in the business of betting or wagering may knowingly accept payment in unlawful internet gambling.[47] The UIGEA defines "bet or wager" as

---

42 *Id.*

43 Gambling, LEGAL INFO. INST., CORNELL U. LAW SCH., https://www.law.cornell.edu/wex/gambling.

44 Thomas Barrabi, *Are Daily Fantasy Sports Legal? DraftKings, FanDuel Federal Regulation Inevitable After Insider Information Leak*, IBT (Oct. 6, 2016, 3:45 PM), http://www.ibtimes.com/are-daily-fantasy-sports-legal-draftkings-fanduel-federal-regulation-inevitable-after-2129333.

45 Unlawful Internet Gambling Enforcement Act (UIGEA) 31 U.S.C.S. § 5361(a)(4) (LexisNexis 2016).

46 *Id.*

47 31 U.S.C.S. § 5363 (2016).

staking or risking by any person of something of value upon the outcome of a contest of others, a sporting event, or a game subject to chance, upon an agreement or understanding that the person or another person will receive something of value in the event of a certain outcome. . .[48]

However, the UIGEA explicitly lists a number of activities that are not considered bets or wagers.[49] One activity that was federally legalized was the participation in any fantasy or simulation sports game, so long as three criteria are met: (1) all prizes offered to winning participants are established and made known to the participants in advance of the game and their value is not determined by the number of participants or the amount of any fees paid (2) all winning outcomes reflect the relative knowledge and skill of the participants and are determined predominantly by accumulated statistical results of the performance of individuals athletes (3) and the scoring system is in no way based on team results.[50]

B. The UIGEA Fantasy Sports Exception May Not Apply to Daily Fantasy Sports

Daily fantasy sports companies such as DraftKings and FanDuel have long maintained that daily fantasy sports fall under the federal exception, and are thus legal.[51] However, this may not be the case for a number of reasons.

The UIGEA does not differentiate between traditional fantasy sports and daily fantasy sports. However, this may not be the case for a number of reasons. The UIGEA does not differentiate between traditional fantasy sports and daily fantasy sports. However, the drafter of the UIGEA had traditional Fantasy Sports, as opposed to daily fantasy sports, in mind when they passed the legislation. Although they passed the UIGEA in

48 *See id.* § 5362(i).

49 *See id.* § 5382(1)(e).

50 *Id.* § 5362(1)(e)(ix)(I)-(III).

51 Barrabi, *supra* note 44.

2006, they did not create the first DFS company until 2009.[52] Also, the drafters of the UIGEA stated that they were not considering daily fantasy sports when they drafted the statute.[53] Former Representative Jim Leach of Iowa, a U.S. Congressman, who drafted the UIGEA in 2006, voiced that lawmakers, including himself, had no idea daily fantasy sports would, "morph into today's cauldron of daily betting."[54] He also stated that the anti-gambling act was supposed to stop internet gambling, not promote it.[55] Thus, if a court were to look to the legislative history of the UIGEA as persuasive, it is plausible that a court could determine that the federal carve out does not apply to daily fantasy sports.

In addition, daily fantasy sports may not meet the criteria afforded by the UIGEA fantasy contest exception. The question in the U.S. remains whether daily fantasy sports are games of skill or games of chance. If they are games of chance, daily fantasy sports would not meet the criteria of the UIGEA, which requires that "[a]ll winning outcomes reflect the relative knowledge and skill of the participants."[56]

However, whether daily fantasy sports falls under the exemption or not, daily fantasy sports competitions must still comply with each individual state's particular prohibitions on gambling.[57] The exemption, under the UIGEA, "does not speak to the operation of a gambling business, simply the flow of funding surrounding the business."[58]

---

52 Futterman, *supra* note 27.

53 Tim Dahlberg, *Former Congressman Says Daily Fantasy Sports Sites Are A 'Cauldron of Daily Betting'*, PBS (Oct. 21, 2015, 6:50 PM), http://www.pbs.org/newshour/rundown/former-congressman-says-daily-fantasy-football-sites-cauldron-daily-betting/.

54 *Id.*

55 Dahlberg, *supra* note 53.

56 UIGEA § 5362(1)(e)(ix)(II).

57 CHRIS GROVE, *Here's the Truth About The Legality Of Daily Fantasy Sports*, LEGAL SPORTS REPORT (Sept. 17, 2015, 11:00 AM), http://www.legalsportsreport.com/3967/are-daily-fantasy-sports-legal/.

58 *Id.*

In addition, the UIGEA is designed to not supersede any other law, including state law.[59] Therefore, even if DFS companies comply with the UIGEA safe harbor, fantasy sports still may violate state law.[60]

IV. Legality of Daily Fantasy Sports on the State Level

Gambling-related activities are regulated in all fifty states. Gambling regulation and prohibition has traditionally been left to the states, and federal gambling laws have been enacted to help states enforce their own gambling laws.[61] Thus, in 2015, daily fantasy sports caught the attention of state Attorney Generals and state legislatures. A number of Attorneys General offices have launched investigation into the daily fantasy sport business mode to determine whether it constitutes illegal gambling.[62] Under state law, the inquiry is still whether the game is one of skill or one of chance.[63] Many argue that daily fantasy sports is a game of chance as opposed to a game of skill, and are thus illegal under individual state's anti-gambling laws.[64] If a state deems daily fantasy sports illegal gambling, DFS company's must either ease operation in that state or risk criminal penalization under that state's anti-gambling laws.[65] A number of notable states have already banned daily fantasy sports because they have determined that it constitutes illegal gambling.

---

59 *Id.*

60 *Id.*

61 Nathaniel J. Ehrman, *Out of Bounds? A Legal Analysis of Pay-To-Play Daily Fantasy Sports*, 22 Sports Law. J. 79, 95 (2015).

62 *See generally*, Nigel Duara, *States crack down on fantasy sports, calling them games of chance, not skill*, Los Angeles Times (Jan. 2, 2016, 12:10 PM), http://www.latimes.com/nation/la-na-ff-fantasy-sports-bans-20160102-story.html.

63 Ehrman, *supra* note 61, at 96.

64 Duara, *supra* note 62.

65 See e.g., *Letter to DraftKings*, New York Times (Nov. 10, 2015), http://www.nytimes.com/interactive/2015/11/10/sports/document-final-nyag-draftkings-letter-11-10-2015.html; *FanDuel Letter*, New York Times (Nov. 10, 2015), http://www.nytimes.com/interactive/2015/11/10/sports/document-final-nyag-fanduel-letter-11-10-2015-signed.html.

Perhaps the most notable state to ban daily fantasy sports is New York. On November 10th, 2015, New York Attorney General Eric Schneiderman, deemed daily fantasy sports as illegal gambling, and told companies to halt accepting bets in the state.[66] The Attorney General's office launched an investigation in October 2015, and the findings revealed a business model more akin to a lottery and that DFS was illegal gambling from a reasonable interpretation of New York Penal laws.[67] The letters also acted as a formal pre-litigation notice to enjoin illegal acts and to obtain additional injunctive relief, restitution, penalties and damages.[68] As of March 21, 2016, DraftKings and FanDuel settled with the New York Attorney General, and were forced to stop operating in New York until the penal laws were amended.[69]

A. State Judicial Tests

In determining whether a game constitutes gambling, states employ different judicial tests. These tests are designed to determine what levels of skill and chance are present in a particular game or contest, and whether those levels are sufficient or insufficient under state law.[70] In regard to daily fantasy sports, no state court in the United States has applied its individual test to determine whether it is a game of chance or skill. However, in applying state judicial tests to daily fantasy sports and predicting how courts will rule in the future, the outcome is not clear-cut.

---

66 *Letter to DraftKings*, *supra* note 65.

67 *Id.*

68 *Id.*

69 Chris Grove, *FanDuel, DraftKings Reach Settlement With New York Attorney General*, Legal Sports Report (Mar. 21, 2016, 9:00 AM), http://www.legalsportsreport.com/9130/fanduel-draftkings-reach-ny-settlement/.

70 Anthony N. Cabot, Glenn J. Light & Karl F. Rutledge, *Alex Rodriguez, A Monkey, and the Game of Scrabble: The Hazard of Using Illogic to Define the Legality of Games of Mixed Skill and Chance*, 57 Drake L. Rev. 383, 390 (2009).

i. Dominant Factor Test

Nearly all states employ the "dominant factor test," otherwise known as the "predominance test."[71] The test is a judicial interpretation of state statutes prohibiting gambling, and turns on whether skill predominates over chance.[72] When chance is an "integral" part that influences the result of a game, chance dominates the game.[73] Chance is not "integral" to the result where skill overrides the effect of the chance.[74] Although chance may be present in a game, its influence cannot be so great as to influence the outcome.[75] For a court to consider skill dominant in a game, skill or the competitors' efforts must sufficiently govern the result. Skill must control the final result, not just on part of the larger scheme.[76] Even games in which skill is a significant, although not a dominant element, the game is forbidden under the test.[77]

The dominant test, although straight-forward, is a difficult test to apply.[78] Claims have been made that courts do not understand the relevance of proffered evidence and have difficulty understanding the different types of change.[79] Also, whether a game is one predominantly of skill or chance is a quest of fact, not of law.[80] Therefore, the results in applying the dominant factor test to mixed-games of skill and chance have been in-

---

71 Steven D. Levitt, Thomas J. Miles, & Andrew M. Rosenfield, *Is Texas Hold 'Em a Game of Chance? A Legal and Economic Analysis* Geo L. J. 581, 588, (2013).

72 *Id.* at 588.

73 *Id.* at 593.

74 *Id.* at 593-94.

75 *Id.* at 594.

76 Levitt, *supra* note 71, at 594.

77 *Id.* at 589.

78 *See generally* Cabot, *supra* note 70, at 402.

79 Cabot, *supra* note 70, at 404-07.

80 *Id.* at 401.

consistent.[81] For example, poker has been described as both a game of chance and skill.[82] Also, in evaluating games with hybrid characteristics, two states have applied the dominant factor test to identical games and came to opposite conclusions regarding whether they were games of skill or games of chance.[83]

ii. Material Element Test

Other states apply stricter tests to determine whether a game is one of chance or skill. The minority approach in the U.S. is the material element test, which has been employed by at least nineteen states.[84] Under the material element test, a court must examine the element of chance by determining whether a particular game contains chance as a material element affecting the outcome of the game.[85] Although skill may primarily influence the outcome of a game, a state that employs this test may prohibit wagering on the game if chance has more than a mere incidental effect on the game.[86]

The material element test is just as difficult, if not more difficult, to apply than the dominant factor test.[87] A court must determine both the level of chance in a particular game and when that level of chance becomes material to the outcome.[88] This is problematic because the word "material" is not defined by statutes in the states that use the test.[89] Also, the word "material" has various meanings, and courts are unsure which meaning to

---

81 *Id.*

82 *Id.*

83 *Id.*

84 Alabama, Alaska, Hawaii, Missouri, New Jersey, New York, Oklahoma, Oregon and Washington. Cabot, *supra* note 70, at 392 n.64.

85 Cabot, *supra* note 70, at 392.

86 *Id.* at 392-93.

87 *Id.* at 402-03.

88 *Id.* at 402.

89 Cabot, *supra* note 70, at 402.

employ.[90] Without one identifiable meaning of what material is, courts will undoubtedly reach different results in determining whether a game is one of chance or skill.

B. Ineffectiveness of State Judicial Tests Regarding Daily Fantasy Sports

As previously mentioned, state judicial tests are difficult to apply. Both the dominant factor test and the material element test are inadequate in that courts may reach different conclusions when applying the same test. In addition, under the material element test, the word "material" is ambiguous, which leads to greater inconsistency.

Therefore, if daily fantasy sports were analyzed under either the dominant factor test or the material element test, there is no telling what the outcome would be. Thus, states should take action to create carve outs for daily fantasy sports instead of leaving them to the fate of inconsistent judicial interpretation.

V. Legal Solutions Recommended to States

As daily fantasy sports come under fire from a number of people and entities, there is remaining uncertainty as to the legality of daily fantasy sports under current state gambling laws. Therefore, states should take action to create daily fantasy sport carve outs in their state laws, and create regulatory and consumer protection frameworks. Only then will state residents be able to play daily fantasy sports in a secure environment, while at the same time benefitting individual states.

A. State Legislatures Should Create Carve Outs for Daily Fantasy Sports In Their State Gambling Laws

In 2015 and 2016, a number of state legislatures took up the issue of daily fantasy sports. In many states, legislative bills have been drafted that seek to legalize daily fantasy sports.[91]

---

90 *Id.* at 403.

91 Dustin Gouker, *Legislative Tracker: Daily Fantasy Sports, Sports Betting*, Legal Sports Report, http://www.legalsportsreport.com/dfs-bill-tracker/ (Last Visited Apr 28, 2017).

One state that is seeking to legalize daily fantasy sports is Missouri.[92] The introduced bill states that the meaning of gambling within the statute "does not include participating in a fantasy contest as defined in this section."[93] The statute defines a fantasy contest as one in which:

> (1) winning participants are eligible to receive cash or anything of value;
> (2) the value of all prizes are established in advance of the contest and;
> (3) no winning outcome is based on the score, point spread, or performance of a single team or athlete.[94]

These requirements are similar to those listed in the UIGEA. Another state legislature that has drafted a bill to legalize daily fantasy sports is New York.[95] Out of a number of bills introduced, Senate Bill 6793, which was drafted by the Racing, Gambling and Wagering Committee in the New York Senate, is likely to be chosen as the bill of choice.[96] In its early stages, a main purpose of the bill was to exempt daily fantasy sports from New York Penal Law forbidding games of chance.[97] Also, discussion and other bill drafts in the New York legislature have suggested amending the state constitution to allow for daily fantasy sports.[98] New York's proposed legislation is particularly important because as of March 21, 2016, DraftKings and FanDuel reached a settlement with the New York Attorney General, who sued the companies because they're business

---

92 *See* S.B. 1045, 98th Gen. Assemb., Reg. Sess., (Mo. 2016).

93 S. Res. 1045 § 572.010 (1).

94 S. Res. 1045 § 572.010 (4)(a) - (d).

95 S. B. 6793 (N.Y. 2016).

96 Dustin Gouker, *Newest Fantasy Sports Bill In New York Is The One To Watch*, Legal Sports Report (Feb. 24, 2016 at 11:10), http://www.legalsportsreport.com/8509/newest-new-york-dfs-bill/.

97 S. B. 6793, § 1502 (N.Y. 2016).

98 Gouker, *supra* note 96.

practices violated New York law.[99] This meant that the sites were to stop operating and taking entries in New York.[100] Thus, without the passage of Senate Bill 6793 or another similar bill, daily fantasy sports will not be allowed to operate within the state.[101]

States should take action to amend their laws through legislation to create carve outs for daily fantasy sports. By creating these carve outs, the state is protecting daily fantasy sports, and all of the benefits that come with them, from old gambling laws and uncertain judicial tests. The bill set forth by the Missouri Senate is an example that state legislatures should use in crafting its own bills. First, the bill specifically and clearly exempts daily fantasy sports from the state's anti-gambling laws. Second, the bill states that daily fantasy sports are exempt so long as certain conditions are met.[102] These conditions, similar to those in the UIGEA, ensure that daily fantasy sports remain games of skill, and continue to be distinguishable from other types of illegal gambling.

Without these legislative carve outs, states may not be able to safe guard daily fantasy sports. Such as in New York, state attorneys general may deem daily fantasy sports illegal under the state's anti-gambling laws, and they would be in serious trouble without legislative action. Therefore, legislative actions taken in states like Missouri, New York, and others, should be mimicked in other states.

B. State Legislatures Should Create Regulatory and Consumer Protection Frameworks

Since the Inception of online daily fantasy sports, DFS companies have operated virtually regulated.[103] As a result, states lose out on a large amount of revenue that could be collected from DFS companies operating within its borders. Also, a large num-

---

99 GROVE, *supra* note 69.

100 *Id.*

101 *Id.*

102 S. RES. § 1045.

103 BARRABI, *supra* note 44.

ber of consumers who participate in daily fantasy sports have not been protected from daily fantasy business practices. Because of this, state legislatures should enact legislation that both regulate daily fantasy sports and protect consumers who participate in them.

i. Regulatory Framework

A number of states have imposed, or are in the process of imposing regulations on daily fantasy sports contests. A Road Island Bill, introduced in February 2016, would further authorize, license, and regulate fantasy sports contests by imposing requirements on licensed operators of fantasy sports games.[104] The act imposes registration fees on these licensed operators, and imposes fines for violating the act.[105]

Another state that has introduced a regulatory bill is California.[106] In 2015, the California legislature proposed the Internet Fantasy Sports Game Protection Act, which is meant to require an entity to apply for and receive a license, and subject those licensed entities to certain regulations.[107] The bill is drafted to:

"(1) ensure that internet fantasy sports games of any duration are offered only in a manner consistent with federal and state law; (2) ensure that the state is able to collect income tax revenues from registered players participating in authorized internet fantasy sports; (3) create systems to protect players private information and prevent fraud and identity theft; (4) to collect annual regulatory fees and deposit them in a Fantasy Sports Fund for the purpose of enforcement efforts; among others."[108]

---

104 H.B. 7492, Gen. Assemb., Reg. Sess., (RI. 2015), *available at https://advance.lexis.com/document?crid=761b3dac-6608-4c88-a1a9-53d786fe913f&pddocfullpath=%2Fshared%2Fdocument%2Fstatutes-legislation%2Furn%3AcontentItem%3A5J1D-9VS0-022F-J0VY-00000-00&pdcontentcomponentid=148786&pdmfid=1000516&pdisurlapi=true.*

105 *Id.*

106 S. Res. 1437, Gen. Assemb., Reg Sess. (Cal. 2015), http://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201520160AB1437.

107 *Id.*

108 S. Res. 1437 § 19754 (a)-(h).

States should adopt regulatory frameworks, using other state approaches as examples. Combined, both Rhode Island and California have comprehensive regulatory ideas that would allow a state to effectively regulate the online daily fantasy sport industry. First, states should require DFS companies to obtain licenses within the state, and pay registration fees in order to fund enforcement efforts. Also, imposing fines for violating the regulations, as well as other state and federal law, is imperative in maintaining effective enforcement. Next, allowing the state to collect income tax revenues from registered players ensures profit for the state that it otherwise would not have obtained. Last, creating systems to prevent fraud and identity theft is important in protecting daily fantasy sport participants. Although other regulations may be warranted, this recommended regulatory framework is a base for states to begin with.

ii. Consumer Protection Framework

In addition, a number of states have drafted consumer protection laws in regards to daily fantasy sports. Because daily fantasy sports are a largely unregulated area, many state legislatures believe it is important to put appropriate safeguards in place to protect consumers.

One state that has drafted consumer protection legislation is Connecticut.[109] The bill was drafted in February 2016, and requires that the Commissioner of Consumer Protection adopt regulations to protect consumers who pay online daily fantasy sports contests form unfair or deceptive acts or practices that may rise in the gaming process.[110] The bill calls for a variety of consumer protections, such as:

"(1) prohibiting daily fantasy sports operators from allowing persons under the age of twenty-one from participating; (2) protections of consumer funds on deposit with daily fantasy sports operators; (3) requirements regarding truthful advertising; (4)

109 S.J. Res. 192, Gen. Assemb., Reg. Sess. (2016), https://www.cga.ct.gov/2016/TOB/s/2016SB-00192-R01-SB.htm.

110 S.J. Res 192 § (1)(b).

procedures to ensure the integrity of all daily fantasy sports contests; and (5) protections for problem gamblers."[111]

Another state that is considering a consumer protection framework is New York.[112] The proposed New York bill has added other important consumer safeguards, such as: (1) employees of the registered company, and relatives living in the same household of such employees, may not compete in any fantasy sport contest; (2) prevent employees of the registered company from sharing confidential information that could affect fantasy sports play with third parties until the information has become public; (3) the participant must be eighteen years or older; (4) restrict players, game officials, coaches, or other participants in a real-world game or competition from participating in daily fantasy games in which he or she is apart of; (5) prevent cheating in the use of software programs that place entry fees or adjust the players selected by a fantasy sports participant; (6) prohibit collegiate sports and horse racing; (7) disclose the number of entries a single fantasy sports contest player may submit and take reasonable steps to prevent players from submitting more than the allowable number; among others.[113]

Other important consumer protections were put forth by the Massachusetts Attorney General in 2015.[114] The Attorney General proposed regulations similar to those of New York and Connecticut, but added even more regulation on problem gamblers.[115] One proposed regulation was to limit deposits to $1,000.00 in a calendar month, less a customer proves that he or she can sustain losses at a higher limit.[116] Also,

---

111 *Id.*

112 S. Res. 6793 (N.Y. 2016), *available at* http://legislation.nysenate.gov/pdf/bills/2015/S6793.

113 S. Res. 6793 §1503.

114 Dustin Gouker, *Massachusetts AG Proposes Sweeping Daily Fantasy Sports Regulations That Will Likely Shift Industry*, Legal Sports Report (Nov. 19, 2015, 7:57 AM), http://www.legalsportsreport.com/6385/massachusetts-ag-dfs-regulation/.

115 *Id.*

116 *Id.*

the AG required that operators must limit the number of entries from a single user based on a siding sale.[117]

States should adopt consumer protection frameworks in order to ensure that consumers may participate in a fair daily fantasy contests. A combination of both Connecticut's and New York's consumer protections, as well as the Massachusetts AG regulations, should be adopted by states in order to adequately protect consumers. First, age limits and limits on gambling addicts are important to ensure irresponsible players are not participating in daily fantasy contests. In addition, by limiting the amount of money and the number of entries an individual may enter, compulsive gambling can seriously be curbed. Second, restricting employees of DFS cites is important to ensure the integrity of each contest and to cut down on cheating and insider trading. Third, by restricting players, game officials and coaches from participating in DFS contests in which he or she is apart of will further ensure the integrity of professional sports by preventing "game fixing." In addition, all other protections in the Connecticut and New York bills, as well as the Massachusetts AG's regulations, are important to ensure that consumers are protected to the utmost extent. Although other protections may be warranted, the recommended list is a comprehensive place for states to begin.

VI. Policy Considerations

There are various policy reasons why state legislatures should take action to allow daily fantasy sports to continue operating within state borders.

A. Daily Fantasy Sports Do Not Present the Same Dangers As Traditional Sports Gambling

Traditional sports gambling has created problems such as corruption, match fixing, and compulsive gambling. However, daily fantasy sports do not present the same dangers as traditional sports gambling does.

---

117 *See id.*

i. Corruption and Match Fixing

A major reason why sports betting became illegal in the U.S. was due to corruption and scandal involving the rigging of sports contests. One early scandal was the infamous Black Sox scandal of the 1919 Major League Baseball World Series.[118] After the Chicago White Sox lost the World Series, eight of the team's players were accused of intentionally throwing the series in exchange for cash.[119] Another early scandal was a point shaving scheme during the 1978-1979 Boston College Men's Basketball season.[120] During the season, gamblers recruited B.C. players to not cover the point spread while playing against other teams, and each player would receive a $2,500 payout in exchange.[121]

In response to scandals in sporting events, preventative laws have been passed over time. One such law was the Professional and Amateur Sports Protection Act (PAPSA), which passed in 1992.[122] The senate report reveals that the committee had concerns for the "integrity of, and public confidence in, amateur and professional sports."[123] The Committee was concerned that widespread legalization of sports gambling would inevitably promote suspicion about controversial plays and lead fans to think 'the fix was in' whenever their team failed to beat the point-spread.[124]

However, corruption and match fixing is not a danger in daily fantasy sports. Daily fantasy sports do not carry the risk of corruption because it is infeasible to fix a

---

118 Dominic Alessi, *Top 10 Sports Betting Scandals and Controversies*, The Richest (June 21, 2014), http://www.therichest.com/sports/top-10-sports-betting-scandals-and-controversies/?view=all.

119 Steussy et al., *supra* note 60, at 20-21.

120 *Id.*

121 *Id.*

122 Nat'l Collegiate Athletic Ass'n v. Governor of N.J., 730 F.3d 208, 215 (2013).

123 *Id.* at 216.

124 *Id.*

fantasy game involving a group of players who are on multiple teams.[125] In daily fantasy sports, the outcomes are based on multiple players' performances in multiple games, rather than the outcome of one specific game.[126] DFS websites requires all entries must be made up of players drawn from a minimum of two sporting events to participate in a contest.[127] Therefore, it would be extremely difficult to be able to influence enough players to change their performance enough to ensure the required outcome.[128] "The structure of fantasy leagues, in which fantasy teams are comprised of different players from each real-world team, does not give any incentive to influence, fix, or tarnish individual games."[129]

ii. Compulsive gambling

Another major reason why sports betting became illegal in the U.S. is due to compulsive gambling.[130] Compulsive gambling is the uncontrollable urge to keep gambling despite the toll it takes on one's life.[131] Compulsive gamblers are often at risk of depleting their savings, accumulating debt, and even resorting to theft or fraud to support their addiction.[132] Typically, it is difficult to curb compulsive gambling by regulatory oversight.[133] In the context of casino gambling, testimony before the U.S. House Judi-

---

125 Brent Schrotenboer, *Leagues see real benefits in daily fantasy sports*, USA TODAY SPORTS (Jan. 1, 2015, 8:35 PM), http://www.usatoday.com/story/sports/2015/01/01/daily-fantasy-sports-gambling-fanduel-draftkings-nba-nfl-mlb-nhl/21165279/.

126 Ehrman, *supra* note 61, at 111.

127 *Terms of Use*, FANDUEL, https://www.fanduel.com/terms (last updated Oct. 28, 2016).

128 Ehrman, *supra* note 61, at 111.

129 Jon Boswell, *Fantasy Sports: A Game of Skill That Is Implicitly Legal Under State Law, and Now Explicitly Legal Under Federal Law*, 25 CARDOZO ARTS & ENT. L.J. 1257, 1274 (2008).

130 *See Compulsive Gambling*, MAYO CLINIC, http://www.mayoclinic.org/diseases-conditions/compulsive-gambling/basics/definition/con-20023242 (last updated Oct. 22, 2016).

131 *Id.*

132 *Id.*

133 *See generally*, Bernard P. Horn, *Is There a Cure for America's Gambling Addiction?*, PBS FRONTLINE, http://www.pbs.org/wgbh/pages/frontline/shows/gamble/procon/horn.html.

ciary Committee revealed that casinos do not want to stop gambling addiction because they can depend on addicts for a huge percentage of their profits.[134]

In the context of daily fantasy sports, excessively wagering money can be curbed by adopting consumer protection laws. These laws, if effective, should identify problem gamblers and limit their wagering on DFS cites.[135] In addition, laws should create limits on how many entries are allowable per individual participant, and a cap on how much money can be wagered. [136] With these safeguards in place, compulsive wagering can be minimized.

B. Legality of Daily Fantasy Sports Would Inhibit Underground Illegal Sports Betting

"Despite legal restrictions, illegal sports betting is wide spread" in the United States.[137] Illegal sports betting is a thriving underground business, with an estimated $400 billion being illegally wagered on sports each year.[138] Despite this fact, illegal sports gambling is operating "free from regulation or oversight."[139]

First, if daily fantasy sports were deemed illegal, participants will likely begin to partake in illegal sports gambling. Widespread popularity of daily fantasy sports indicates that there is a wide desire and acceptance to wager money on sport performance. Without providing daily fantasy sports as a legal outlet to do so, individuals will resort to underground illegal gambling through bookmakers. This illegal practice has no oversight, and puts individuals in danger of unrestricted financial loss, establishing gambling problems, and betting at a young age.

134 *Id.*

135 *See* S. Res. 6793, § 1503 (N.Y. 2016) (enacted).

136 Gouker, *supra* note 114.

137 Adam Silver, *Legalize and Regulate Sports Betting*, GENIUS (2016), http://genius.com/Adam-silver-legalize-and-regulate-sports-betting-annotated.

138 *Id.*

139 *Id.*

Second, by deeming daily fantasy sports illegal, daily fantasy sports will not cease to continue, but instead will be forced underground or even oversees. According to Michelle Minton, a consumer policy fellow at the Competitive Enterprise Institute:

"When online gambling was largely considered illegal in the United States, Americans still spent billions of dollars wagering on websites operated overseas. That's what will happen if daily fantasy sports betting is thrown back into the black market: Most will continue to play online but in a much less secure environment."[140]

Therefore, the better solution that states should employ is to legalize daily fantasy sports and create a safe and secure environment for individuals to participate. By doing this, states can inhibit underground and overseas betting.

C. Legality of Daily Fantasy Sports Would Generate Revenue and Jobs

If daily fantasy sports were legalized and regulated by states legislatures, a large amount of tax revenue could be generated. As previously stated, $400 billion is illegally wagered on sports each year.[141] Consequently, illegal wagering does not generate any revenue or create jobs. In contrast, in the United Kingdom, the government generated 1.7 billion pounds in tax revenue from gambling in 2012-2013.[142] In addition, the UK gambling industry has employed over 100,000 people.[143]

By legalizing daily fantasy sports and creating regulatory and consumer protection frameworks, states can begin to generate revenue. States would do so by collecting income tax revenues from registered players and taxing daily fantasy sites at an appro-

---

140 Gabrielle Cintorino, *State Lawmakers Call Foul on Daily Fantasy Football*, The Heartland Institute (Dec. 9, 2015), https://www.heartland.org/news-opinion/news/state-lawmakers-call-foul-on-daily-fantasy-football.

141 Silver, *supra* note 137.

142 Heitner, *supra* note 1.

143 *Id.*

priate rate.[144] Because there is a rough projection that the DFS market will generate $14.4 billion in revenue by the year 2020, states would greatly benefit by taxing the sites.[145] However, by taxing DFS companies too much, it could be problematic for the sites, especially those that do not generate as much revenue as DraftKings and FanDuel.[146] One recommended rate is a ten percent tax, which would only tax the administrative fees of the DFS contests.[147] Additionally, daily fantasy sports can create jobs by the sites employing individuals, and by the state employing individuals to enforce new regulations.

D. Popularity of Daily Fantasy Sports Indicates Widespread Acceptance of Wagering on Athletic Performance

As indicated earlier, popularity of daily fantasy sports has surged since the creation of DraftKings and FanDuel.[148] According to the Fantasy Sports Trade Association, 56.8 million people play fantasy sports in the U.S. and Canada as of January 2016.[149] Daily fantasy sports have increasingly become a popular and accepted form of entertainment in the United States, and wagering on DFS contests may be indicative of a changing attitude in the country.

Also, it is indicative that professional sports leagues, which have long lobbied against wagering on sports, are investing heavily in daily fantasy sports.[150] Professional leagues understand that viewers want to partake in daily fantasy sports, and that the

144 John Mehaffey, *What A Regulated Daily Fantasy Sports Industry Might Look Like*, Legal Sports Report, (Oct. 1, 2015, 7:58 AM), http://www.legalsportsreport.com/4393/regulating-daily-fantasy-sports/.

145 *See* Wong, *supra* note 3.

146 Mehaffey, *supra* note 144.

147 *Id.*

148 *See* Heitner, *supra* note 1.

149 *Industry Demographics*, FTSA, http://fsta.org/research/industry-demographics/ (last visited Feb. 9, 2017).

150 *See* Heitner, *supra* note 1.

leagues can profit greatly off of their legality.[151] Leagues recognize they can turn consumers' love of fantasy contests into "higher ratings, more viewership and engage fans during non prime-time games."[152]

Conclusion

With the recent surge in popularity of online daily fantasy sports, the question remains whether DFS companies are operating legally or illegally. Since daily fantasy sports have been brought to the legal forefront in the U.S., many believe that DFS companies are providing games of chance, as opposed to games of skill. In order to ensure that daily fantasy sports can operate legally in individual states, state legislatures should take action to legalize daily fantasy sports, while creating regulatory and consumer protection frameworks. Only in this way will state residents be able to participate in daily fantasy sports in a secure environment, while at the same time benefitting individual states.

151 *See id.*

152 *Id.*

Bridging the (Information) Gap: Reconciling and Re-Codifying State and Federal Personal Data Policy

Samuel Drew Miller[1]

ABSTRACT

This paper intends to introduce the prior and current state of personal data at the state and federal level, as very few people are aware of the amount and kinds of personal data which can be collected. The first section of this paper will provide case studies of two States, Massachusetts and California; accompanying these case studies will be statues, as well as cases which highlight how the courts have approached and interpreted the issue of personal data collection, use, and security. The second section of this paper will then shift the focus toward the federal government, highlighting how the federal government has interpreted the issue of personal data through legislative history and Supreme Court cases. Next, I will propose a federal statute regulating the use, security, and collection of personal data. Following the introduction of the proposed statute, I will also apply a comparative analysis between the respective cases and statutory language to the proposed legislation. Finally, this note will discuss how the realm of personal data use, collection, and security may change as society continues to evolve.

1 Syracuse University College of Law, Juris Doctor Candidate 2017. Special thanks to Professor Aviva Abramovsky for her encouragement and guidance throughout the development of this note. Finally, a special thanks to my fellow members of the Syracuse Journal of Science and Technology, whose continuous support and motivation made this possible.

I. *INTRODUCTION*

In the 21st Century, it is virtually impossible to operate within society without either giving personal data or having your personal data used by corporations or the government. Many people are unaware to the sheer amount of personal data which is given and shared among agencies and corporations. Personal data means "data which relate to a living individual who can be identified - (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual."[2] The definition of personal data is inherently a generalized and broad definition. At its core, it is meant to cover any information that relates to identifiable, living individuals. There are different ways in which an individual can be considered identifiable; for example, a person's full name would be a likely obvious identifier. International law, such as the Data Protection Directive, has recognized a person can also be identifiable from other information, including elements such as physical characteristics, pseudonyms, occupation, and addresses.[3] However, it needs to be considered and recognized that data may become personal from information that could come into the possession of a data controller.[4]

Furthermore, it is interesting to note that it there are hardly any restrictions relating to how personal data may be stored. Although there have been many attempts to codify and re-define the scope of personal data, both the legislative and judiciary have been slow to adapt their understanding. The issue here is whether, based on continuously changing definitions and collection methods of personal data, as highlighted through

2 Alasdair Taylor, *What Is Personal Data*, SEQ LEGAL (Feb. 17, 2011, 11:40 AM), http://www.seqlegal.com/blog/what-personal-data.

3 *What Is Personal Data?*, OFFICE OF THE DATA PROTECTION COMMISSIONER, https://www.dataprotection.ie/docs/What-is-Personal-Data-/210.htm (last visited Sep. 30, 2016).

4 *Id.*

state and federal statutes, a new standard should be implemented to create clear and non-restrictive means for public and private entities to utilize personal data.

Alternatively, there also does not exist a comprehensive federal law regulating the collection, use, and security of personal data does not exist. In other words, this paper asks whether there should there be a uniform standard for which the courts can determine if and how the use of personal data should be collected and/or utilized be adopted? This paper shall argue for the adoption of such a standard. I believe there should be such a standard, and this paper will attempt to craft such a standard.

Part I in this paper will shall introduce you to the concept of personal data and illustrate recent developments surrounding the collection and utilization of personal data. Part II will contain an introduction to the background and history of state use of personal data, and will offer a comparative analysis of two states, California and Massachusetts, to observe how different states have attempted to resolve the issue. The scope of Part III will shall focus on the federal government's interpretation of personal data and its use by analyzing statutory law and federal court cases. In Part IV, I will introduce a proposal for a newly-crafted federal statute pertaining to the re-defining of personal data, as well as setting forth regulations for its collection and use. Finally, Part V will reconciles the previous case studies by applying the language of the proposed legislation, followed by analytical commentary as to the benefits of this proposed statute, as well as a brief conclusion.

II. *PART I: WHAT IS PERSONAL DATA: A BRIEF HISTORY, OVERVIEW, AND CURRENT ISSUES*

A. *What is Personal Data?*

Personally identifiable information ("PII"), another term for personal data, is information that can be used on its own or with other information to identify, contact, or

locate an individual.[5] PII is also defined as any information about an individual maintained by an agency.[6] This can include (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.[7] Examples of PII include, but are not limited to, the use of names such as full name, maiden name, or alias; a personal identification number, such as social security number (SSN); address information, such as street address or email address, and personal characteristics, including photographic images, fingerprints, or other biometric data.[8] Federal statutes, regulations, and memorandum for federal departments and agencies require certain sectors, such as healthcare, financial, federal public sector, and the Department of Veterans Affairs to implement security programs for information and provide notification of security breaches of personal information.[9]

B. *Current Landscape and Issues*

In the United States, there is no single, comprehensive federal law regulating the collection, use, and security of PII; instead, the United States has a collection of multiple federal and state laws and regulations.[10] Oftentimes, these laws and regulations end up overlapping, contradicting, or nullifying language in the respective statutes.[11] Forty-sev-

---

5 Erika McCallister, Tim Grance & Karen Scarfone, *Computer Security Division: Guide to Protecting the Confidentiality of Personally Identifiable Information* (PII), National Institute of Standards and Technology (2010), *available at* http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf.

6 *Id.*

7 *See id.*

8 McCallister, *supra* note 5.

9 Gina Stevens, Cong. Research Serv., Data Security Breach Notification Laws, R42475 (2012).

10 Ieuan Jolly, *Data Protection in United States: Overview*, Practical Law (July 1, 2016), http://us.practicallaw.com/6-502-0467.

11 *See* Jolly, *supra* note 10.

en states have enacted legislation requiring private, governmental, or educational entities to notify individuals of security breaches of information involving personally identifiable information.[12] Additionally, "thirty-one states have enacted laws that require entities to destroy, dispose, or otherwise make personal information unreadable or undecipherable."[13] The Federal Trade Commission's Disposal Rule also requires proper disposal of information in consumer reports and records to protect against unauthorized access to, or use of, the information.[14] Unfortunately, because there does not exist a single, comprehensive federal law regulating the collection, use, and security of PII, courts and legislatures are often left to their own devices to understand and interpret personal data use and collection.

According to a Congressional Research Service report, by 2012 over 2,676 data breaches and computer intrusions involving 535 million records containing PII have been disclosed by organizations such as data brokers, businesses, educational institutions, government and military agencies, healthcare providers, and financial institutions.[15] As a result, a large number of individuals have received notices that their PII was improperly disclosed.[16] Given the troubles already posed by individuals, professional 'hacker' organizations, and in rare cases, corporations and government organizations, the disclosure and security of personal data is a critical issue. With no clear definition of PII, it remains likely this issue will continue to persist until definitions begin to harmo-

12 Pam Greenberg, *Security Breach Notification Laws*, National Conference of State Legislatures (Jan. 4, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx. (States with no security breach law: Alabama, New Mexico, and South Dakota).

13 Pam Greenberg, *Data Disposal Laws*, National Conference of State Legislatures (Jan. 12, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx.

14 *Disposing of Consumer Report Information? Rules Tells How*, Fed. Trade Comm'n (2005), https://www.ftc.gov/tips-advice/business-center/guidance/disposing-consumer-report-information-rule-tells-how.

15 Stevens, *supra* note 9.

16 *Id.*

nize with the current system, and protective measures can be implemented to protect these interests.

III. *PART II: STATE INTERPRETATION: CASE STUDIES ON PERSONAL DATA COLLECTION, USE, AND SECURITY*

State security breach notification laws typically follow a framework, and can be categorized into several standard elements.[17] The most common elements are:

> "(1) delineating who must comply with the law; (2) defining the terms "personal information" and "breach of security"; (3) establishing the elements of harm that must occur, if any, for notice to be triggered; (4) adopting requirements for notice; (5) creating exemptions and safe harbors; (6) clarifying preemption and relationships to other federal laws; and (7) creating penalties, enforcement authorities, and remedies."[18]

In the following sections, two states (California and Massachusetts) will be analyzed through these elements, comparing both statutory language and case law. Ultimately, I will compare these two case studies together, then seek to develop the best elements of the law from each state to further develop the proposed legislation.

These two States have been chosen for a variety of reasons. As of 2012, California has the largest population among the 50 states, composed of nearly 38 million people.[19] Furthermore, due to its geography, economy, and population makeup, California has traditionally served as a representative sample for the United States; indeed, many policies and new ideas find their roots in California. Additionally, the issues pertaining to personal data have a particular resonance within California because the state is associated with technological innovation and the birth of the personal computer. Finally,

17 *Id.* at 5.

18 Stevens, *supra* note 9, at 5.

19 UNITED STATES CENSUS BUREAU, https://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?src=bkmk.

California serves as an excellent example of a state attempting to resolve the issues surrounding the 21st century conceptualization of personal data because of its comprehensive statutory authority regarding personal data and security measures, as well as recent changes the state has made to these statutes.

Massachusetts was chosen for its unique focus toward PII. First, the state offers an east-coast perspective on the issues surrounding personal data. Next, Massachusetts has a unique perspective toward the maintenance and protection of personal information being one of the central hubs for health services within the country. Furthermore, Massachusetts was one of the first states to augment its legislation surrounding personal data, with substantive changes coming to the previous statutes. Finally, Massachusetts sought to craft laws with an eye toward data security breaches, which offers a foundational basis for which the proposed federal legislation will seek to achieve. For these reasons, Massachusetts offers an interesting perspective on personal data worthy of analysis.

A. *California*

Since the collection of personal data began, states have attempted to regulate the means by which data may be collected, as well as additional provisions for the use, protection, and destruction of personal data. In California, the statutes pertaining to personal data are some of the most comprehensive regulations nationwide. California was the first jurisdiction to enact a data breach notification law in 2002, requiring notification when unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.[20] In California, any business which fits within the state's statutory definition may collect personal information.

Cal. Civ. Code § 1798.80[21]

---

20 STEVENS, *supra* note 9, at 3.

21 CAL. CIV. CODE § 1798.80 (Deering 2016).

Under Cal. Civ. Code § 1798.80, a business is defined as

> a sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the law of this state, any other state, the United States, or of any other country, or the parent or the subsidiary of a financial institution.[22]

Personal information means "any information that identifies...a particular individual, including, but not limited to, his or her name, signature, social security number, physical characteristics or description".[23] Records of personal information mean "any material...on which information is recorded or preserved".[24] California's definition of records "does not include publicly available directories containing information an individual has voluntarily contented to have publicly...listed".[25] Additionally, ""personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records."[26]

Cal. Civ. Code § 1798.16[27]

Another statutory provision, Cal. Civ. Code § 1798.16, relates to the maintenance of personal data collectors, as well as the access to the information.[28] In California, "whenever an agency collects personal information, the agency shall maintain the source...of the information", unless the source is the subject of the data, or the subject has

---

22 Cal. Civ. Code § 1798.80 (Deering 2016).

23 *Id.*

24 *Id.*

25 *Id.*

26 *Id.*

27 Cal. Civ. Code § 1798.16 (Deering 2016).

28 *See id.*

received a copy of the source document.[29] This includes "the name of any source who is an individual acting in his or her own private or individual capacity".[30] Additionally, with regards to the accessibility of the sources, Cal. Civ. Code § 1798.16 states that the agency "shall maintain the source...of the information in a readily accessible form, so as to be able to provide it to the data subject when they inspect any record," unless the agency is considered to be exempt from disclosure.[31]

Cal. Civ. Code § 1798.40[32]

Furthermore, another statute, Cal. Civ. Code § 1798.40, discusses the disclosure of personal data and information when dealing with the individual for which the information pertains.[33] In essence, this section of the California Civil Code sets forth the exceptions for which an agency is exempt from disclosing PII. For example, the first three exceptions listed deal with information gathering in criminal investigations.[34] Additionally, exceptions are granted to agencies when dealing with individuals serving in the public sector, as well as exemptions granted under what appears to be an interest in workplace health and compensation.[35]

Recent Changes: Cal. Civ. Code § 1798.81.5[36]

Recently, California enacted changes to its personal data legislation; as of January 1st, 2016, Cal. Civ. Code § 1798.81 was amended to redefine the scope of personal

29 *See id.*

30 *See* Cal. Civ. Code § 1798.16.

31 *See id.*

32 Cal. Civ. Code § 1798.40 (Deering 2016).

33 *Id.*

34 *Id.*

35 *See id.*

36 Cal. Civ. Code § 1798.81.5 (Deering 2016).

information, which would fall under the personal data legislation.[37] In the amended statute, the definition of "personal information" will include: "(a) a username or e-mail address combined with a password or security question and answer for access to an online account; and (b) health insurance information."[38] The amendment also goes on to define what applicable health insurance information includes, such as policy numbers, unique identifiers used by health insurers, and information pertaining to claims and application history.[39] In effect, the amendment to the statute requires holders of personal information to establish reasonable security measures for protecting that information. The amendment seemingly seeks to harmonize the new definitions of personal data with California's data notification breach law, Cal. Civ. Code § 1798.82.

Cal. Civ. Code § 1798.82[40]

Cal. Civ. Code § 1798.82 states that:

> A person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery of the breach in the security of the data to the individual whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."[41]

Additionally, Cal. Civ. Code § 1798.82 establishes when a breach occurs, "the person or business which was responsible for maintaining that data shall promptly notify the owner of the information of the breach."[42] Furthermore, under Cal. Civ. Code §

37 *See* CAL. CIV. CODE § 1798.81.5.

38 *See id.*

39 *See id.*

40 CAL. CIV. CODE § 1798.82 (Deering 2016).

41 *Id.*

42 *See* CAL. CIV. CODE § 1798.82.

1798.82, "the security breach notification shall be written in plain language...and present the information related to the release of the personal data under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information.""[43] Soon after California enacted this law, numerous federal and state bills modeled after the California law began imposing notification requirements on entities that own, license, or process personal information.

The issues of personal data collection, use, and breaches have been adjudicated at the state level for decades; however, as the definition of personal data evolves, the judicial process has struggled to keep up. Furthermore, as the definitions as to what qualifies as personal data change, so do the methods in which personal data can be stored, accessed, and utilized. Here too, we find that courts have been traditionally slow to reflect these changes. This is, in all fairness, probably not the fault of the courts; indeed, the judicial process simply moves at a slower pace than that of the world of commercialization and technology. Below are three cases in which the courts were faced with difficult decisions as to who may hold personal data, the justifications for collecting and using personal data, as well as the competing interests between collectors and original owners of personal data.

Case 1: *Commission on Peace Officer Standards & Training v. Superior Court*[44]

Here, a newspaper petitioned for a writ of mandate, seeking to compel the release of the names and certain identifying employment data pertaining to peace officers throughout California pursuant to the California Public Records Act (PRA).[45] The court concluded that the records at issue were not rendered confidential by Pen. Code, §§ 832.7 & 832.8, and that the records did not come within any of the exemptions con-

43 *See id.*

44 Comm'n on Peace Officer Standards & Training v. Superior Court, 165 P.3d 462 (Cal. 2007).

45 *Comm'n on Peace Officer Standards & Training*, 165 P.3d at 465.

tained in the PRA.[46] Additionally, the court concluded the privacy and safety interests of peace officers in general did not outweigh the public's interest in the disclosure of the information sought by the newspaper.[47]

The court concluded that the information the petitioner, the Commission on Peace Officer Standards and Training, was ordered to disclose was not considered personal data within the meaning of Code, § 832.8, subdivision (a).[48] The court reasoned there was no indication the legislature, in adopting Code sections 832.7 and 832.8, was concerned with making confidential the identities of peace officers or the basic fact of their employment.[49]

This case, decided in 2007, offers a 21st century approach to the complexities of the release of PII. In particular, this case is tailored to the release of PII of public servants. As was previously noted in the statutory section, California Civil Code section 1798.40 sets forth an exception regarding individuals engaged in public service. Due to the function of public individuals, namely to serve the interests of the community which they represent, we might expect PII relating to these individuals to be made public.

However, were these individuals considered private citizens acting outside the scope of their employment, we would probably expect a higher level of protection. Indeed, protections afforded to the privacy of private citizens are a cornerstone in the foundation of our country. It is essential to recognize that, with public servants, there may always be contention addressing whether they are acting as private citizens or as public servants. However, in the context of the First Amendment, the courts have traditionally considered public servants to be separate from private citizens. Though the question may arise as to when an individual would cease to be a public servant and

46 *See id.* at 467-68.

47 *See id.* at 477.

48 *See id.* at 472.

49 *See id.*

return to the realm of private citizenry, I believe California adopted the correct position on this matter.

Case 2: *International Federation of Professional & Technical Engineers, Local 21, AFL-CIO v. Superior Court*[50]

Staying within the realm of individuals employed within the public sector, this next case offers a different illustration about information that may be released upon request. Here, the trial court ordered a city to disclose the salary information of all city employees who earned $100,000 or more in the fiscal year 2003-2004, pursuant to a petition by real parties in interest, the newspapers.[51] In its holding, the California Court of Appeals concluded that the names and salaries of public employees earning $100,000 or more per year, including peace officers, were not exempt from public disclosure under the California PRA.[52] The court reasoned that disclosure of the salary information at issue would not constitute an unwarranted invasion of personal privacy.[53] The court went on to illustrate that, to the extent that some public employees might expect their salaries to remain private, that expectation was not a reasonable one.[54] Perhaps the principle rationale for the court's decision was that the city and unions failed to present any evidence establishing that the city's consistent past practice of disclosing its employees' salaries created any safety or privacy problems for those employees that would outweigh the public interest in disclosure.[55]

This case offers an example of when and how the California courts will apply the balancing test set forth by Government Code, section 6254, subdivision (c). Un-

50 *Int'l Fed'n of Prof'l & Tech. Eng'rs, Local 21, AFL-CIO v. Superior Court*, 165 P.3d 488 (Cal. 2007).

51 *Int'l Fed'n of Prof'l & Tech. Eng'rs*, 165 P.3d at 491.

52 *Id.*

53 *Int'l Fed'n of Prof'l & Tech. Eng'rs*, 165 P.3d at 493.

54 *See id.* at 494.

55 *See id.* at 498.

der this code, the balancing test states that the customs, practices, and physical settings surrounding particular activities may create or inhibit reasonable expectations of privacy.[56] The California courts have considered a reasonable expectation of privacy to be an objective entitlement founded on general and widely accepted community norms.[57] Here, the employees' interests in avoiding the disclosure of their salaries was outweighed by the public's interest in knowing how its representative government was spending its money.

Furthermore, when comparing the rationale behind the *Peace Officers* case to this decision, it becomes important to consider the facts surrounding the cases. In *Peace Officers*, all that was being disclosed were the names of public servants. Here, the courts have gone further in permitting the disclosure of personal information by releasing the salaries of city employees. In the next case, we will see another circumstance in which the courts had to balance the interests of personal information collectors and parties seeking access to the information in order to substantiate claims of discrimination in the workplace.

Case 3: *Alch v. Superior Court*[58]

In *Alch v. Superior Court*, television writers served subpoenas on third parties, seeking data from which they could prepare a statistical analysis to support their claims of age discrimination.[59] A privacy notice was sent to guild members, advising them of their right to object to disclosure of personal information on privacy grounds.[60] The court concluded that the trial court abused its discretion when it sustained all objections

56 *See id.* at 494.

57 *Id.*

58 *Alch v. Superior Court*, 82 Cal. Rptr. 3d 470 (Cal. Ct. App., 2008).

59 *Alch*, 82 Cal. Rptr. 3d at 474.

60 *See id.* at 475-76.

to the disclosure of the requested information on privacy grounds.[61] The court also found the trial court erred in its purported balancing of the objectors' privacy rights and the countervailing interests of the litigants and the state.[62] Continuing its dissection of the lower court's decision, the court also reasoned that the lower court failed to analyze the types of information requested, while further failing to consider the state's interest in preventing discrimination.[63]

Additionally, the court held that the lower court erroneously concluded that the writers could proceed with a statistical analysis supporting their discrimination claim without the information from the objectors.[64] The court came to this conclusion by determining the writers could not prove their claims without access to the personal information, from which they could perform the statistical analysis necessary to corroborate their claims.[65] Finally, the court reasoned the writers further demonstrated that the requested information they sought was directly relevant to their claims and essential to a fair resolution of their lawsuit.[66]

This case offers a great example of a situation where the request of individuals to refrain from having personal data released was denied. In this case, there are two key principles which the court highlights as being central to claims surrounding personal information. The first principle states that "[a party seeking disclosure of personal information from third parties must show they] have a compelling need for the [data], [and by showing the information] is 'directly relevant' and 'essential to a fair resolution' of the[] lawsuit."[67] The second principle illustrates that in evaluating privacy claims in the

61 *See id.* at 478.

62 *See id.* at 482-83.

63 *Id.*

64 *Alch*, 82 Cal. Rptr. 3d at 484.

65 *Id.* at 486.

66 *Id.* at 483-84.

67 *Id.*

context of discovery:

> considerations which will affect discretion include: (1) the purpose of the information sought; (2) the effect that disclosure will have on the parties and on the trial; (3) the nature of the objections urged by the party resisting disclosure, and; (4) the ability of the court to make an alternative order which may grant partial disclosure.[68]

These two principles are just some of the examples courts use for guidance when deciding whether to disclose or preserve PII, and limitations of the kinds of PII that can be disclosed. Going forward, this will require increased judicial understanding of PII and other cyber-based foundational knowledge. Unfortunately, courts have been traditionally slow to adapt to rapidly evolving technologies; therefore, while influential, the judiciary is just one tool in reforming the realm of PII.

1. *Conclusion*

With each case, we see the court interpreting statutory authority, and in some cases, applying judicially created balancing tests in order to determine whether the disclosure of personal information is appropriate. Furthermore, there exists a trend which suggests the courts are fairly deferential toward permitting the disclosure of PII, though the courts and the legislature have attempted to preserve exceptions and limitations to the kinds of PII which can be disclosed. As the California legislature continues to attempt to modify and modernize its statutes, considerations must also be made for the privacy interests citizens possess. In addition, courts must also balance the interests of disclosure of PII and the privacy concerns of the data subjects. As California continues to grapple with these challenges, they continue to serve as a practical example for how other states, as well as the federal government, may wish to proceed. In the next case study, I will analyze how another state, Massachusetts, has attempted to resolve ques-

68 *Id.* at 481.

tions of PII endemic to its citizens, and the challenges which arise from striking a balance between the interests highlighted by California.

B. *Massachusetts*

The Massachusetts security breach, data destruction, and security regulations are considered to constitute some of the most comprehensive sets of general security regulations seen at the state level.[69] These laws and regulations are said to be closely modeled after aspects of developing data security law.[70] The state of Massachusetts had codified the collection, use, and protection of personal data into a comprehensive, yet confusing, statute. However, at the beginning of the 21st century, Massachusetts amended its personal data and personal data security laws, which have come to serve as a leading example for other states looking to update their personal data statutes.[71] In Massachusetts, "personal information includes names, social security numbers, driver's license numbers...or financial account numbers, such as credit card numbers."[72] One of the most interesting, and illustrative, aspects of the new regulations mandate that "personal information be encrypted when stored on portable devices, or transmitted wirelessly or on public networks."[73] Additionally, the regulations call on businesses and individuals who store personal information to utilize up-to-date firewall protections, which only permits authorized users to access or share data.[74]

Mass. Ann. Laws ch. 66A, § 2[75]

---

69 STEVENS, *supra* note 9, at 4.

70 *See id.*

71 Maura Healey, Standards for the Protection of Personal Information of Residents of the Commonwealth, THE OFFICIAL WEBSITE OF THE ATTORNEY GENERAL OF MASSACHUSETTS (Last Visited Mar. 24, 2016), http://www.mass.gov/ago/doing-business-in-massachusetts/privacy-and-data-security/standards-for-the-protection-of-personal.html.

72 Healey, *supra* note 71.

73 *Id.*

74 *Id.*

75 MASS. ANN. LAWS ch. 66A, § 2 (LexisNexis 2016).

Mass. Ann. Laws ch. 66A, § 2 states that every holder maintaining personal data shall conform to several regulations. Sections (a) and (b) relate to identifying people in charge of maintaining personal data systems, as well as requirements on employers to inform those chosen to maintain personal data systems of the rules and regulations surrounding personal data collection.[76] Additional measures, such as those mentioned in section (c), ensure other agencies or individuals not employed by the holder will not have access to personal data.[77] These agencies shall not have access to personal data, "unless such access is authorized by statute or regulations which are consistent with the purposes of this statute, or possession has been approved by the individual whose personal data is sought."[78] Language from section (d) illustrates the antiquated language and understanding of personal data, which limited the scope of the statute to merely physical threats. However, the legislature has attempted to modernize its regulations as new understandings of PII emerge. For example, in 2007, the Massachusetts legislature amended section (d) to include the crime of identity theft.[79]

Mass. Ann. Laws ch. 214, § 3B[80]

The next regulation, Mass. Ann. Laws ch. 214, § 3B, details the State of Massachusetts' attempt to award actual and/or punitive damages in cases where personal data is misused.[81] Specifically,

> "where a defendant ha[s] materially or willfully misused any personal data required to be disclosed to the [individual] according to the provisions of chapter 66-A, and said personal data so misused is material

76 *See* MASS. ANN. LAWS ch. 214, § 3B.

77 *Id.*

78 *Id.*

79 *Id.*

80 MASS. ANN. LAWS ch. 214, § 3B (LexisNexis 2016).

81 *Id.*

to the establishment of the defendant's liability to the [individual], the action may be brought at any time within three years after such misuse is discovered."[82]

As times have changed the scope of PII, however, Massachusetts has attempted to recodify the laws which pertain to the use, collection, and security of PII.

201 CMR 17[83]

The more recent adaptations of Massachusetts's personal data laws illustrate some of the changes the legislature has made to accommodate the technological changes in society. Massachusetts statute 201 CMR 17.00 outlines the standards for the protection of personal information for Massachusetts residents. The objective of 201 CMR 17.00 is to "insure the security and confidentiality of customer information, protect against anticipated threats to the security of personal information, and protect against unauthorized use of personal information that may result in substantial harm to any consumer within Massachusetts."[84]

Furthermore, 201 CMR 17.03 establishes the standards for protecting personal information for residents of Massachusetts; it requires that "every person that owns personal information related to a resident of Massachusetts shall develop, implement, and maintain a security program and contains administrative, technical, and physical safeguards."[85] The statute mandates that "every information security program include measures such as security policies, reasonable restrictions upon physical access to records containing personal information, and disciplinary measures for violations, including possible termination and compensatory damages."[86]

82 Mass. Ann. Laws ch. 214, § 3B.

83 201 Mass. Code Regs. 17.00 (LexisNexis 2016).

84 201 Mass. Code Regs. 17.01 (LexisNexis 2016).

85 201 Mass. Code Regs. 17.03 (LexisNexis 2016).

86 201 Mass. Code Regs. 17.03.

Massachusetts also has an extensive adjudicative history with the issues pertaining to personal data. In each case, the courts have been asked to interpret the Massachusetts statutes in order to determine what kinds of PII are discoverable, and who may obtain control over PII. In Massachusetts, the courts have attempted to balance the interests between protecting the interests of those who maintain PII, and those who seek access, or restriction, to such information. In the next three cases, I will analyze how the Commonwealth of Massachusetts has attempted to resolve these interests, while also attempting to maintain modern applicability to evolving issues surrounding PII.

Case 1: *Allen v. Holyoke Hospital*[87]

In this case, a child was removed from the biological mother's home and placed in foster care.[88] The foster mother subsequently brought the child to the hospital where he died from septic shock.[89] The mother filed a wrongful death action against the hospital. Subsequently, the hospital raised the defense of contributory negligence by the mother for deficient care and nurturing of the child.[90] The hospital sought records from the Department of Social Services that related to the removal of the child from the biological mother. In turn, the biological mother sought a protective order in opposition to the discovery request.[91] Here, the court concluded investigative records from the Department of Social Services that contained information from the child's grandparents and foster parents were privileged information and that it could not determine whether the social worker's recorded observations were privileged until a finding was made as to whether the information was an invasion of the mother's privacy.[92]

---

87 Allen v. Holyoke Hospital, 496 N.E.2d 1368 (Mass. 1986).

88 *Allen*, 496 N.E.2d at 1369-70.

89 *Id.*

90 *Id.* at 1370.

91 *Allen*, 496 N.E.2d at 1370.

92 *See id.* at 1374.

This case offers a good analysis of the Fair Information Practices Act ("FIPA"). Here, the court had to determine whether the record sought was protected by FIPA. This determination depended upon whether the record is a public record pursuant to Mass. Ann. Laws ch. 4, § 7.[93] In this case, the court applied the definition of personal information current to the time of the decision, with the exception that such information was not contained in a public record. However, there became a concern as to when social workers should have access and use of personal information, especially with regards to ensuring public health and safety. The section of the Massachusetts Statute that illustrated this point, Mass. Ann. Laws ch. 66A, § 2(k), does not require that the records be disclosed, but in fact admits a possibility that the records may not be disclosed if the data subject objects to disclosure.[94] It is important to note, however, that the court did allow for a social worker to testify regarding her observations.[95] Whether this adequately served to balance the interests between DSS and private individuals, however, remains to be seen.

Case 2: *Torres v. Attorney General*[96]

In this case, the defendant, an Assistant Attorney General, a party in the plaintiff's federal court action, received a case file from the Department of Social Services ("DSS") containing information that had been collected on plaintiff while he was a client of DSS.[97] The plaintiff, Jose Torres, contended that the disclosure of information by DSS violated the Fair Information Practices Act ("FIPA"), Mass. Ann. Laws, Ch. 66A, and the trial court agreed.[98] The court held that under FIPA, no other agency and no

93 *Id.* at 1372-73.

94 *Id.* at 1373 (*citing* MASS. ANN. LAWS ch. 66A, § 2).

95 *Id.* at 1374.

96 Torres v. Attorney Gen., 460 N.E.2d 1032 (Mass. 1984).

97 *Torres*, 460 N.E.2d at 1033.

98 *Id.* at 1033-34.

individual who was not employed by the agency which held the personal information was allowed to access plaintiff's personal data, unless authorized by statute or approved by plaintiff.[99] The court held that the type of data collected by DSS was personal data in which plaintiff had an expectation of privacy, and was not the type of information available as part of the public record.[100] Furthermore, the court found that because there existed statutory provisions for the data subject to collect exemplary damages, even where damages were not being sought, the DSS would be required to pay Torres for its intrusion onto his privacy.

This case offers an additional analysis of FIPA, especially when compared to the previous case. Here, as in *Allen*, the court gave substantial weight to the right of the individual in determining whether the DSS could utilize personal information. In both instances, the data subject raised objections, and the court cited the language in Mass. Ann. Laws, ch. 66A in upholding the respective objections. This case further serves to illustrate the importance Massachusetts will provide to the rights of the data subjects to object to their PII being used.

Moreover, both cases involved situations where the agency sought to use the personal information against the data subject; it appears as though the courts have been reluctant in permitting such actions. These are important protections; however, arguments can be made that these provisions inhibit the government from performing their full duties, especially with regards to providing for the public health and safety. Although the government does have an obligation to promote the public health and safety of its citizens, those obligations should not interfere with the liberties of the citizens the government is charged to protect. Accordingly, statutes such as Mass. Ann. Laws, Ch. 66A and 201 CMR 17.00 are vital for the protection of individual's rights.

---

99 *Id.* at 1035, 1038.

100 *Id.* at 1037-38.

Case 3: *Amato v. Dist. Attorney for the Cape and Islands Dist.*[101]

Here, as part of a murder investigation, the plaintiff Keith Amato voluntarily provided a deoxyribonucleic acid ("DNA") sample based on promises made by the District Attorney. This promise was made through police detectives acting on his behalf that the sample and its related data would not be retained or used if his DNA did not match the biological evidence from the crime scene.[102] Thereafter, although the District Attorney orally represented to Amato that his DNA sample had been destroyed, the crime lab informed Amato that it had his biological sample, and could not release or destroy the sample or the associated records without the District Attorney's authorization.[103]

The appellate court found that while Amato's biological sample was returned, the crime lab continued to hold the records against his wishes.[104] Additionally, the court held that a statutory requirement that an agency could not maintain more personal data than would be reasonably necessary demands that the agency not continue in possession of personal data when doing so is no longer reasonably necessary.[105] Therefore, the court determined that Amato's allegations that the District Attorney's office continued to hold records related to his DNA sample without his consent, and therefore was in breach of promises of limited use and retention, and for breach of contract.[106]

This case serves as a more modern example of how courts are choosing to review personal data, as well as how courts are applying the language from statutory law pertaining to damages and equitable relief. It should be noted that in *Amato*, the court specifically resisted an analysis into the legislative history; rather, the court found

---

101 Amato v. Dist. Attorney, 952 N.E.2d 400 (Mass. App. Ct. 2011).

102 *Amato*, 952 N.E.2d at 403.

103 *Id.* at 404-05.

104 *Amato*, 952 N.E.2d at 406.

105 *Id.* at 407-08.

106 *Id.* at 406.

that the plain meaning of the term 'personal information' was unambiguous. This is an important aspect the court will undertake when attempting to understand and rectify issues within statutory interpretation. An argument for the alternative holding would be that there are inherent ambiguities within statutes; indeed, if the issues are being adjudicated before the court, there must be some level of ambiguity. This, however, fails to consider the intent of the legislative language. There must be terms and definitions which are commonly understood to mean what we would imagine them to mean; otherwise, our language system would seemingly collapse upon itself!

1. *Conclusion*

Overall, these cases serve to illustrate the protective measures Massachusetts has implemented to protect its citizens, protections which should be implemented on a federal level. In *Holyoke*, the court grappled with the definition of PII as deemed relevant for the purposes of FIPA. More importantly, the court applied the laws relevant to PII to the realm of social workers. As government workers handling sensitive information and sensitive cases, there inherently exists a necessity for a balance between protecting PII of the data subject, while also maintaining public health and general welfare. Similar issues were raised in *Torres*; both cases further serve to illustrate the importance Massachusetts provides to the rights of data subjects to object to their PII being used. *Allen* serves as a more modern example of how courts are choosing to review PII, as well as how courts are applying the language from statutory law pertaining to damages and equitable relief. Ultimately, both California and Massachusetts serve as influential examples of how courts and legislatures should grapple with PII; the challenge is applying these examples to the federal government.

IV. *PART III: FEDERAL INTERPRETATION: PERSONAL DATA AT THE FEDERAL LEVEL*

The legal and regulatory framework for the protection of personally identifiable

information is complex because businesses, governments, and individuals who process data must comply with the requirements of many differing privacy, information security, and breach notification laws.[107] Federal statutes, regulations, and memorandum for federal departments and agencies require certain sectors, such as healthcare, financial, and the federal public sector to implement security programs for information and provide notification of security breaches of personal information.[108] However, at the federal level in the United States, there is no singularly comprehensive statute regulating the use, collection, and maintenance of PII.[109] Rather, the United States utilizes a mix of federal and state statutes.[110]

Unfortunately, this creates overlapping and sometimes contradictory regulations and decisions.[111] In addition, there is no single regulatory authority specifically assigned to oversee data protection in the United States. In contrast to state determinations of PII, there is no single definition of PII; rather, PII is interpreted more broadly than at the state level, and often left to specific acts to define the scope and applicability of PII. At the federal level, different requirements apply to different industries and data processing activities. Because of this, these laws often are narrowly tailored and address specific data uses.[112] While addressing specific issues of PII, this lack of general applicability leads to

---

107 STEVENS, *supra* note 9, at 7.

108 STEVENS, *supra* note 9, at 7.

109 Jolly, *supra* note 10.

110 *Id.*

111 *Id.*

112 Aaron P. Simpson, *Data Protection & Privacy in 26 Jurisdictions Worldwide*, GETTING THE DEAL THROUGH, 191-97 (2014), https://www.hunton.com/files/Publication/1f767bed-fe08-42bf-94e0-0bd03bf8b74b/Presentation/PublicationAttachment/b167028d-1065-4899-87a9-125700da0133/United_States_GTDT_Data_Protection_and_Privacy_2014.pdf.

contradiction, inconsistency, and critical gaps in the protection of citizen's PII.

In this section, I will analyze federal statutes which have attempted to regulate issues pertaining to personal information. These statutes will illustrate how the federal government has attempted to regulate and implement policy pertaining to personal information use, collection, and security. Furthermore, these statutes will indicate how matters pertaining to personal information are to be addressed and redressed. Next, I will then analyze federal court decisions pertaining to the application and interpretation of these statutes, as well as their State counterparts. These cases will indicate the manner in which the courts consider personal information. Furthermore, these cases will highlight some of the challenges courts have had to grapple with in modernizing themselves to evolving standards and definitions of personal information use, collection, maintenance, and security breaches.

A. *Statutes*

15 U.S.C.S. § 45: Unfair methods of competition unlawful; prevention by Commission[113]

15 U.S.C.S. § 45, also known as Section 5 of the Federal Trade Commission Act, is a federal consumer protection law that prohibits unfair or deceptive practices.[114] Flowing from its impact on commerce, this statute has been applied to offline and online privacy and data security policies.[115] Under 15 U.S.C.S. § 45(n), unfair practices are defined as "those that cause or likely to cause substantial injury to consumers which is not reasonably avoidable by consumers and not outweighed by countervailing benefits to consumers or to competition."[116] This statute allows the Federal Trade Commission ("FTC") to enforce consumer protection through administrative and judicial process-

113 15 U.S.C.S. § 45 (LexisNexis 2016).

114 Jolly, *supra* note 10.

115 *Id.*

116 15 U.S.C.S. § 45(n) (LexisNexis 2016).

es.[117] The FTC has used its authority under Section 5 to bring many privacy enforcement actions for alleged violations by entities whose information practices have been deemed unfair.[118] This statute grants the FTC the authority to make the determination as to whether a violation has occurred through the processes of adjudication and rulemaking, or through judicial enforcement.[119]

Under the adjudicatory process, the Commission may issue a complaint setting forth its charges when there is reason to believe that a violation has occurred.[120] If the respondent elects to settle the charges, it may sign a consent agreement without admitting liability, consent to entry of a final order, and waive all right to judicial review. "If the respondent elects to contest the charges, the complaint is adjudicated before an administrative law judge ("ALJ")."[121] Upon conclusion of the hearing, the ALJ issues an initial decision, which sets forth his findings of fact as well as his conclusions of law, and recommends either entry of an order to cease and desist or dismissal of the complaint.[122]

Rather than go through the adjudicatory process, the FTC may utilize regulatory trade rules to remedy unfair or deceptive practices. Under Section 18 of the FTC Act, the FTC is authorized to prescribe "rules which define with specificity acts or practices which are unfair or deceptive acts or practices in or affecting commerce," within the meaning of Section 5(a)(1) of the Act.[123] This method allows the FTC to promulgate remedies in the form of damages. According to the FTC, once the FTC has promulgated

---

117 *A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*, Federal Trade Comm'n (2008), https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority.

118 Simpson, *supra* note 112, at 191.

119 Federal Trade Comm'n, *supra* note 117.

120 *Id.*

121 *Id.*

122 *Id.*

123 15 U.S.C.S. § 57(a) (LexisNexis 2016).

a rule, anyone who violates the rule "with actual knowledge or knowledge fairly implied on the basis of objective circumstances that such act is unfair or deceptive and is prohibited by such rule" is liable for civil penalties.[124]

15 U.S.C. § 6801: Gramm-Leach-Bliley Act ("GLB")[125]

The Gramm-Leach-Bliley Act regulates the collection, use and disclosure of financial information.[126] Under 15 USCS 6801(a), "it is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."[127] In addition, under 15 USCS 6801(b), each financial institution "shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards: (1) to insure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer."[128]

Furthermore, the GLB Act applies broadly to financial institutions and other businesses which provide financial services and products.[129] The GLB Act limits the disclosure of non-public personal information, and in some cases requires financial institutions to provide notice of their privacy practices and an opportunity for data subjects to opt out of having their information shared.[130] Compliance under the GLB Act is man-

124 *See* 16 C.F.R § 1.98 (2016).

125 15 U.S.C.S. § 6801 (LexisNexis 2016).

126 Jolly, *supra* note 10.

127 15 U.S.C.S. § 6801 (LexisNexis 2016).

128 *Id.*

129 15 U.S.C.S. § 6801 (LexisNexis 2016).

130 *Id.*

datory for financial institutions; under the GLB Act, there must be policies in place to protect information from reasonably foreseeable threats in security and data integrity.[131] Additionally, financial institutions are required to provide you with a notice of their information-sharing policies when you first become a customer, and annually thereafter.[132] That notice must inform the consumer of the financial institutions' policies on disclosing nonpublic personal information ("NPI") to affiliates and nonaffiliated third parties, disclosing NPI after the customer relationship is terminated, and protecting NPI.[133]

42 U.S.C. §1301: Health Insurance Portability and Accountability Act ("HIPAA")[134]

The Health Insurance Portability and Accountability Act, also known as HIPAA, primarily regulates health information. HIPAA applies broadly to a multitude of industries, including health care providers, data processors, pharmacies and other entities that come into contact with medical information.[135] In addition, HIPAA also revised the Security Breach Notification Rule 45 C.F.R. Part 164, which requires covered entities to provide notice of a breach of protected health information.[136] Under the new revision, an entity must provide notice of acquisition, access, use, or disclosure of protected health information in a manner not permitted under the Privacy Rule.[137]

As evidenced through each of these statutes, there are numerous efforts to regulate the use, collection, maintenance, and security of personal information. However, due to the current multitude of statutes, the current statutory authorities are overly complex,

131 *Id.*

132 *The Gramm-Leach-Bliley Act*, *supra* note 131.

133 *Id.*

134 42 U.S.C.S. § 1301 (LexisNexis 2016).

135 *Supra*, text accompanying note 131.

136 *Id.*

137 45 C.F.R. 164 (LexisNexis 2016).

confusing, and too compartmentalized. An argument could be made that having individual agencies administer their own regulations for personal information allows for more individualized protections specific to the information at issue. However, this inherently creates less cooperation between agencies, and often leads to contradictory promulgations and interpretations of personal information issues. Unfortunately, because there is no one agency that possesses exclusive domain over personal information matters, courts are oftentimes left to interpret statutes across a wide spectrum of agencies.

In the next section, the two cases decided by the Supreme Court illustrate how the court has interpreted personal information within the realm of the federal courts. The first case will revolve around the Freedom of Information Act, which provides citizens the right for the government to disclose information it possesses. In the second case, a more modern case, the courts must grapple with modern technology and answer questions regarding access to personal information through these mobile devices.

B. Cases

United States DOJ v. Reporters Comm. for Freedom of Press[138]

In *United States DOJ v. Reporters Comm.*, news groups and an association of journalists sought the disclosure of any criminal records in the possession of the Federal Bureau of Investigations ("FBI") and the Department of Justice ("DOJ") pertaining to allegations of congressional corruption under the Freedom of Information Act ("FOIA").[139] The FBI denied the request to disclose the criminal records of the living subjects, but agreed to disclose the information for the deceased subject.[140] One of the central issues surrounding this case was the issue of privacy; indeed, the court recognized the privacy interest in a criminal record was substantial.[141] To resolve the matter,

138 *United States DOJ v. Reporters Comm. for Freedom of Press*, 489 U.S. 749 (1989).

139 *Id.* at 757.

140 *See id.*

141 *Id.* at 771.

the court had to determine whether an invasion of privacy was warranted.[142] The court then utilized a balancing test of sorts, which stated that "whether an invasion of privacy was warranted had to turn on the nature of the requested document, and its relationship to the basic purpose of FOIA, which focused on the citizen's right to be informed about the government's actions."[143]

Here, the court stated that the groups did not intend to discover anything about the conduct of the agency, and response to the request would not shed any light on the agency's conduct.[144] Perhaps more importantly, the court generalized that this would presumably be the case in which one private citizen is seeking information about another agency.[145] Therefore, the court rationalized that the public interest in the release of a criminal record was not the type of interest intended to be protected by the FOIA.[146] In addition, a third party's request for law enforcement records about a private citizen could reasonably be expected to invade that citizen's privacy, and that when the request sought no official information about the government, the privacy invasion was unwarranted.[147]

This case offers us an opportunity to observe how the Supreme Court considered requests for personal information and data outside of the digital age. At the same time, the matter over which the issue surrounded, the criminal record, has been and will continue to be a source of contention in the realm of personal information. Many interested parties, including journalists, private citizens, and law enforcement officials, have a substantial interest in the disclosure (or non-disclosure) of this kind of sensitive infor-

142 *Id.*

143 *See United States DOJ*, 489 U.S. at 771-72.

144 *See United States DOJ*, 489 U.S. at 773.

145 *Id.*

146 *Id.* at 775.

147 *Id.* at 780.

mation. Of note should be the balancing test utilized by the Supreme Court. As noted earlier in the California case study, the court in *International Federation of Professional & Technical Engineers, Local 21, AFL-CIO v. Superior Court* also applied a balancing test to determine whether personal data was subject to disclosure. In *International Federation of Professional & Technical Engineers*, the court's application of the balancing test provided significant deference to the subjects of personal data. Here, the court also recognized the privacy rights of data subjects; at the same time, the court also gave government agencies protections against the disclosure of some of its actions.

Riley v. California[148]

In *Riley v. California*, a consolidation of two separate cases, two defendants were arrested by law enforcement.[149] In both cases, the law enforcement officers seized the defendants' cell phones; in each case, the officers also obtained information through the use of the cell phones to eventually connect the defendants to other criminal activities.[150] Following the charges, both defendants sought to suppress the evidence on Fourth Amendment grounds.[151] Chief Justice Roberts highlighted the issue: "whether the police may, without a warrant, search digital information on a cell phone seized from an individual who has been arrested."[152] The Supreme Court held that the police officers generally could not, without a warrant, search digital information on the cell phones seized from the defendants as incident to the defendants' arrests.[153]

In its holding, the court opined that, while the officers could examine the phones' physical aspects to ensure that the phones would not be used as weapons, dig-

148 Riley v. California, 134 S. Ct. 2473 (U.S. 2014).

149 *Id.* at 2477.

150 *Id.*

151 *See id.*

152 *See id.* at 2480.

153 *Riley*, 134 S. Ct. at 2477.

ital data stored on the phones could not itself be used as a weapon to harm the arresting officers or to effectuate the defendant's escape.[154] Furthermore, the potential for destruction of evidence by remote wiping or data encryption was not shown to be prevalent and could be countered by disabling the phones.[155] Moreover, the immense storage capacity of modern cell phones gave rise to privacy concerns, especially with regard to the extent of information which could be accessed on the phones.[156]

Because phones possess the possibility to document some of the most private aspects of an individual's private life, there exist concerns over the possibility of broad invasions of privacy. Indeed, the court cites statistics indicating the substantial amount of private information individuals keep stored on their cell phones.[157] As Chief Justice Roberts notes:

> "The storage capacity of cell phones has several interrelated consequences for privacy. First, a cell phone collects in one place many distinct types of information that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even just one type of information *to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier.*"[158]

This case indicates that, as reliance on mobile technology continues to permeate

154 *See Riley* at. at 2478.

155 *See id.* at 2486-87.

156 *See id.* at 2489.

157 *Id.*

158 *Id.*

society, the amount of personal information contained on these mobile devices also increases. As the court in *Riley* indicated, there are needs to protect this information. Furthermore, with developments in data storage ever-changing, the access and protection of this data becomes of paramount concern. One such question that arises deals with who may access this data, and what kinds of data may be accessed through non-conventional means. Recently, a debate arose as to whether the government could compel one of these corporations - Apple, Inc. - to develop an operating system through which the government could access data encrypted on cell phones. As the court noted, the destruction of evidence through wiping or data encryption was not prevalent. However, as society has increasingly shifted toward such technology, questions will inevitably arise as to whether the government has the ability to access encrypted data.

PART IV: PROPOSED STATUTE

Preamble and Scope

The proposed statute has taken into consideration case decisions from the Supreme Court. In addition, the proposed statute has considered relevant case law from the two case studies from Massachusetts and California. Perhaps most importantly, this proposed statute has captured the critical components from the state statutes, as well as elements from the various federal statutes. The statute has four critical elements: Scope of Statutory Authority; Maintenance of Personal Information; Security Breaches and Other Breaches of Personal Information; and Damages and Redressability. When analyzing the state and federal statutes, as well as relevant case law, it became apparent that these sections were of critical importance in the realm of personal information. The purpose of this statute is to provide a federal minimum that all states shall conform to, while providing a regulatory agency to ensure these minimums are met. The definitions and regulations are intentionally general; states should maintain the authority to best prescribe the laws pertinent to the needs of their citizens.

Section 1: Definitions

1) For the purposes of this statute,
    a) 'Data Breach' shall refer to the unauthorized access or use of unencrypted personal information, encrypted personal information with reasonable means of compromising the encryption of said information, or compromised security of physical, tangible documents related to personal information which creates a reasonably likely risk of fraud or theft.
        i) In cases of agency action, a data breach shall be considered to have occurred where the agency fails to obtain the consent of the data subject, or fails to discard of personal information in conformity with this statute.
    b) 'Data Collector' shall refer to any person which stores, maintains, or utilizes personal information.
    c) 'Data Subject' shall refer to the original individual as to whom the data belongs.
    d) 'Person' means any individual, corporation, or other legal entity, other than an agency connected or associated with the government.
    e) 'Personal Information' means any information that can be used to identify, associate, or describe a person. Examples of personal information shall include, but are not limited to, general information (name, address, telephone number, email addresses, etc.), social security numbers, passport numbers or other federal identification cards, health care or insurance information, and financial or banking information.
    f) 'Record(s)' means any material upon which information is recorded or maintained, whether in physical, digital, or other forms.

Section 2: Scope of Statutory Authority

1) This statute shall apply to all businesses, agencies, private entities, healthcare facilities, and third-party storage providers which collect, use, maintain, sell, or otherwise utilize personal information data on individuals which possess the rights afforded as

citizens by the United States Constitution.

2) The Department of Commerce shall possess the following responsibilities:

a) Oversight:

i) The Department of Commerce shall delegate oversight of its personal information duties to a sub-agency under the jurisdiction of the Department of Commerce. This agency shall be responsible for monitoring and ensuring compliance with this statute and updating the relevant House and Senate Commerce committees.

(1) The Department of Commerce and its applicable subcommittee(s) shall adhere to the Administrative Procedure Act ("APA") in regards to judicial review.

b) Regulation and Enforcement:

i) The Department of Commerce shall have principal authority to update statutory language as the appropriate standards of personal information continue to evolve. The Department of Commerce and its applicable sub-committee(s) shall adhere to the APA in compliance with its rulemaking and adjudicatory authority.

(1) This statute explicitly requires the Department of Commerce and its applicable subcommittee(s) to utilize formal adjudication and rulemaking in its procedures.

c) Claim Redressability:

i) The Department of Commerce and its applicable subcommittee(s) shall establish regulations pertaining to the redressability of claims resulting from data breaches.

(a) Section 4 shall dictate the appropriate standards for addressing data breaches.

(b) Section 5 shall dictate the permissible damages data subjects may

seek as a result of a data breach.

3) In exceptional circumstances, and with the explicit consent with the Department of Commerce, other executive agencies may assume similar responsibilities possessed by the Department of Commerce.
    a) In order to classify as an exceptional circumstance, the agency requesting personal information shall demonstrate to the Department of Commerce the following criteria:
        i) A direct connection between the personal information and the scope of the agency's principle objectives;
        ii) A detailed overview regarding the following information:
            (1) Scope of the authority sought;
            (2) Duration of the time the authority is sought; and
        iii) Detailed constraints illustrating the methods by which the agency shall collect, use, maintain, and discard personal information.
    b) Explicit consent may be granted by the Department of Commerce in the following manners:
        i) Written consent, detailing the scope and purpose of the responsibilities afforded to the requesting agency;
        ii) Electronic consent, detailing the scope and purpose of the responsibilities afforded to the requesting agency; or
        iii) Oral communications, under the following circumstances, may constitute origins of explicit consent which may lead to delegation of authority where there exists:
            (1) Notification and documentation of the original oral communication;
            (2) Additional oral communications made following the original communication; and
            (3) A final record of the oral communication detailing all communications

between interested parties subject to the agreement.

Section 3: Maintenance of Personal Information

1) Maintenance
    a) Digital Personal Information:
        i) The data collector shall establish secure, independent servers for the collection and maintenance of personal information. The data collector shall keep record of the source of the data, a detailed description of the data, as well as the method by which the personal information was obtained.
    b) Tangible or 'hard-copy' Personal Information:
        i) The data collector shall create secured storage facilities for the collection and maintenance of personal information. The data collector shall have the authority to categorize the personal information, subject to the oversight and regulations imposed by the Department of Commerce.
2) Statute of Limitations for Collecting or Maintaining Personal Information
    a) Following a period of five (5) years, the Department of Commerce or other regulatory agency shall be subject to section 3.5 of this statute.
        i) Exceptions: The following circumstances shall be exempt from the statute of limitations for collecting or maintaining personal information:
            (1) Records intended to assist law enforcement officials in criminal investigations;
            (2) DNA or biometric data; and
            (3) Medical information or other relevant information that would be used to the detriment of the data subject.
        ii) Should the personal information fall within the exceptions clause of this subsection, the data collector shall dictate a fair and reasonable statute of limitations for the collection or maintenance of personal information.
3) Disposal of Personal Information

a) Digital Personal Information:

i) The data collector shall take all necessary steps to ensure proper disposal of all personal information under its control when:

(1) The statute of limitations has expired and exceptions have not been granted; or

(2) Maintenance and possession of personal information is deemed by the Department of Commerce as no longer necessary.

ii) When the requirements of subsection (i) have been met, the data collector shall digitally erase, wipe, encrypt, or otherwise delete all electronic records of the personal information.

b) Tangible or 'hard-copy' Personal Information:

i) The data collector shall take all necessary steps to ensure proper disposal of all personal information under its control when:

(1) The statute of limitations has expired and exceptions have not been granted; or

(2) Maintenance and possession of personal information is deemed by the Department of Commerce as no longer necessary.

ii) When the requirements of subsection (i) have been met, the data collector shall physically destroy all personal information, except under the circumstances listed in subsection (3)(a)(i) of this section.

<u>Section 4: Security Breaches and Other Breaches of Personal Information</u>

1) Digital Breaches of Personal Information

a) In the event of a data breach, the data collector shall adhere to the following subsections.

b) The data collector, upon determining a breach has occurred, shall undertake the following actions:

i) Promptly notify the data subject;

ii) Provide the data subject with a comprehensive notice regarding:

(1) The cause of the breach;

(2) The extent of the breach;

(3) A detailed explanation and analysis pertaining to the efforts of the data collector in illustrating what actions they are taking; and

(4) A detailed explanation and analysis pertaining to what actions the data subject should do.

iii) Provide the Department of Commerce or relevant agency with notice of the data breach.

c) Following notification of a data breach, the Department of Commerce shall:

i) Provide the data subject with any additional information regarding the data breach;

ii) Conduct an investigation on the methods utilized by the data collector; and

iii) Provide recommendations to the data collector and data subject on how to proceed going forward.

2) Tangible Breaches of Personal Information

a) In the event of a data breach, the data collector shall adhere to the following subsections.

b) The data collector, upon determining a breach has occurred, shall undertake the following actions:

i) Promptly notify the data subject;

ii) Provide the data subject with a comprehensive notice regarding:

(1) The cause of the breach;

(2) The extent of the breach;

(3) A detailed explanation and analysis pertaining to the efforts of the data collector in illustrating what actions they are taking; and

(4) A detailed explanation and analysis pertaining to what actions the data

subject should do.

iii) Provide the Department of Commerce or relevant agency with notice of the data breach; and

iv) Conduct an internal investigation regarding the data breach.

c) Following notification of a data breach, the Department of Commerce shall:

i) Provide the data subject with any additional information regarding the data breach;

ii) Conduct an investigation on the methods utilized by the data collector; and

iii) Provide recommendations to the data collector and data subject on how to proceed going forward.

Section 5: Damages and Redressability

1) Subject to a data breach, the data controller shall be liable to the data subject where the following elements can be proved:

a) The data breach occurred;

b) The data was maintained by the data controller; and

c) The data subject suffered harm from the release of personal information.

i) Harm need not be physical nor limited to theft or fraud.

2) If the elements of subsection (1) are proven, the data subject shall have redressability in the form of actual and punitive damages.

a) If punitive damages are to be awarded, the damages are not to exceed a fair and reasonable amount proportional to the harm suffered.

3) In the case of a data breach, the data collector shall be liable to pay a fine no less than one hundred dollars ($) per data subject affected by the data breach.

PART V: APPLICATION AND ANALYSIS

At the federal level, there does not exist a singular statute that specifically provides protections, regulatory authority, and remedies for data subjects. Furthermore, there is no single agency that explicitly possesses jurisdiction over personal information.

With this proposed statute, the federal government would now possess regulatory authority over personal information through the Department of Commerce. Moreover, one of the principle objectives in crafting a federal personal information statute is balancing the scope and authority between the state and federal government. While recognizing the need for federal oversight, the principle authority to regulate personal information should lie at the state and local level. Because these levels of government maintain much more communication with the populace, these governments are best equipped to recognize and manage the needs of their citizens.

When comparing the language of the proposed statute to the relevant case studies and statutes, there were designed similarities drawn from the respective statutes of Massachusetts and California. For example, Section 5 of the proposed statute, Damages and Redressability, drew significant influence from MASS. ANN. LAWS ch. 214, § 3B. In particular, Massachusetts provided a detailed statutory provision through which victims of data breaches could recover damages. Additionally, the statute instituted penalties for data collectors who failed to protect the information of their subjects. At the federal level, there should also exist similar redressability measures; by providing a minimum for damages, this will encourage states to follow suit with their respective statutes.

Furthermore, following the FTC Act, HIPPA, and GLB Act, the principle objective following the respective federal statutes was to create a centralized statute directly under the authority of one executive agency. However, noting the necessity for inter-agency collaboration, the proposed statute creates avenues for which other agencies can assume regulatory responsibility. In addition, the proposed statute creates an additional level of oversight by way of communicating with congressional committees in order to increase transparency and uniformity.

CONCLUSION

As the United States enters the height of the 21st century, the need for feder-

al protections regarding personal information use, collection, and security remains a critical issue. As states such as California and Massachusetts attempt to recodify and restructure their statutes, courts have also had to adapt their understanding of PII. Specifically, as new realms of PII are realized, and the necessity for protecting and securing PII becomes a focal point, states and legislatures must adapt to the ever-changing world around them. In the federal system, without the assistance of the proposed legislation, the applicability and protective measures of case law and statutes shall remain inherently limited. With a general federal statute, the federal government is more apt to provide basic assurances to all citizens, regardless of whether states have enacted legislation. Finally, by providing for the proper use, regulation, collection, security, and redressability for PII, the federal government will have the ability to ensure basic rights and protections for the citizens for which they are sworn to serve.

Blockbuster Drugs: The Rise and Decline of the Pharmaceutical Industry

Reviewed by: William Salage

Citation: Jie Jack Li, Blockbuster Drugs: The Rise and Decline of the Pharmaceutical Industry (2014).

Relevant Legal and Academic Areas: Biomedical Research, Drug Industry History, Drug Industry Trends, Drug Therapy History, Intellectual Property Law, Patent Litigation, Pharmaceutical Preparations.

Summary: Dr. Jie Jack Li provides a comprehensive analysis of the blockbuster drug industry in the United States. The author defines the four major therapeutic fields in which blockbusters exist: the treatment of ulcers, antihistamines, blood thinners, and pain management. In each of these categories the author provides detailed case studies of the scientific discoveries, business decisions, marketing campaigns, and court cases which lead to blockbuster success for each drug. The author identifies the current problems with the blockbuster model and possible solutions both the government and pharmaceutical industry itself can take to continue the great medical, chemical, and biological innovation, as well as the financial success, which has defined the pharmaceutical industry over the past century.

About the Author: Dr. Jie Jack Li is currently an Associate Professor of Chemistry at the University of San Francisco. Before his independent academic career, he spent fifteen years in drug discovery at "big pharma" including Pfizer and Bristol-Meyers Squibb Company. He is the author of *Triumph of the Heart: The Story of Statins* (Oxford University Press, 2009), *Modern Organic Synthesis in the Laboratory* (Oxford University Press, 2007), and *Laughing Gas, Viagra, and Lipitor: The Human Stories Behind the Drugs We Use* (Oxford University Press, 2006).

I. Introduction

In the book, *Blockbuster Drugs: The Rise and Decline of the Pharmaceutical Industry*, author Jie Jack Li explores the expansion of the pharmaceutical industry and its relationship to the unprecedented success of a small number of drugs. Li examines the traditional therapeutic areas in which blockbuster drugs exist and why fewer blockbusters have come to market over the past decade. Finally, Li explores what reforms might be done to continue to develop the blockbuster business model.

II. The Blockbuster Defined

Blockbuster drugs are medications with sales over $1 billion. Li defines three elements that contribute to the success of most blockbusters. The first of these elements is achieving high sales by designing drugs which treat a large patient population. In other words, finding the largest market with the greatest demand. Blockbusters typically treat one of six common illnesses: hypertension, high cholesterol, pain, ulcers, allergies, or depression.

Secondly the drug must go beyond being merely an effective treatment. The drug must also be efficient and have minimal side effects. For example, many older tricyclic anti-depressants required patients to undergo a long course of treatment and have severe side effects because these antidepressants were non-selective targeting drugs and thus caused collateral damage in the patient's body. As such, many patients were unable to complete the full course of treatment because of the side effects, which in many cases were unavoidable, resulting in fewer physicians prescribing the drug, and therefore fewer patients using the drug.

Finally, Li identifies marketing as the last key element of a successful blockbuster drug. Marketing brings the drug to the attention of both the public and proscribing physicians. In other words, marketing and a strong sales force brings the drug to the targeted market.

III. Blockbuster Model

Blockbuster drugs have permeated the global marketplace and have saved and improved the lives of millions. Much of the financial success of pharmaceutical industry owes to the simple blockbuster business model, which is as follows: pharmaceutical companies rep enormous profits from creating blockbuster drugs and treating the major ailments of the world. In turn, large portions of the profits from past blockbusters were reinvested into the research and development of new blockbusters. As the author notes, "looking for new ones [blockbusters] that will sustain the 'life cycle' for the health of both the patients (physical and mental) and the drug companies themselves (financial)." Therefore, pharmaceutical companies must produce drugs to keep its customers alive who in turn provide the financial capital necessary to keep the pharmaceutical company financially alive.

IV. Blockbuster Drugs

The author, in great detail, examines the discovery and business models of the major blockbuster drugs over the past three decades.

A. *The First Blockbuster*

Tagamet was the world's first blockbuster when it reached sales of $1 billion in 1996 and by 2000, grossed over $140 billion worldwide. Tagamet was discovered through cooperation between James Black and Smith Kline & French (SK&F). Tagamet treated peptic ulcers through the use of anti-hysterectomies. Before Tagamet, the only treatment for peptic ulcers was bed rest and a bland diet. Tagamet was relatively simple for patients to take, only requiring a regimen of one to four pills a day for about six to eight weeks. The Food and Drug Administration (FDA) approved Tagamet in 1977. By 1979, Tagamet was marketed in over 100 countries as it represented a solution to the global problem of stomach ulcers.

The high demand for Tagamet led SK&F to pursue new manufacturing methods in order to create larger quantities of the drug. The initial method to prepare Tagamet used lithium aluminum hydrate (LAH) for the reduction of an imidazole ester intermediate. However, the use of LAH was problematic. LAH was dangerous as it could create a large exothermic reaction, was expensive to operate, and LAH was in limited supply. SK&F thus invested in an alternative to the LAH process and discovered the Birch reduction method, saving millions of dollars in manufacturing costs. More importantly, the Birch reduction also provided process patent protection and therefore enhanced its [Tagamet's] market exclusivity in countries around the world. Therefore, SK&F could both significantly decrease the manufacturing costs of Tagamet, and secure stronger market exclusivity for years to come, ensuring a long lasting and steady income stream, which could be redirected towards research and development.

Despite the additional process patent protection held by Tagamet, SK&F conducted clinical trials for the FDA in order to gain approval for an over-the-counter, generic version of Tagamet to sell once patent protection expired. The author notes such a precaution was well founded, as sales of Tagamet dropped from $600 million in 1993, to $400 million in 1994, a $200 million loss in profit after losing patent protection.

B. Continued Treatment of Ulcers

While Tagamet revolutionized the treatment of ulcers, it was not perfect. As the author notes in the book, blockbusters are characterized by their efficiency in treating patients and simplicity in providing a cure. The problem with Tagamet was its long treatment period and short half-life, as it required patients to take the drug up to four times a day. Moreover, Tagamet had minor side effects, such as the occurrence of skin rashes or sexual dysfunction in males. Therefore the market was ripe for another blockbuster to treat ulcers that was both more efficient and with fewer side effects.

The answer came in the form of Glaxo's Zantac. Zantac was discovered in

1976, which was largely due to SK&F's "remarkably non-secretive publication of their preliminary results" for Tagamet. In 1972, David Jack, the inventor of Zantac, attended a lecture by James Black, where Black "revealed that burimamide not only inhibited histamine-induced acid secretion in animals and humans, but also worked on acid secretion following food ingestion." Jack then immediately began researching burimamide. The result was Zantac, which only needed to be taken once per day, was selective in its binding mechanism resulting in fewer drug on drug interactions, and did not produce sexual dysfunction in males.

Without the side effects associated with Tagamet, Zantac easily gained market share. Additionally, Glaxo priced Zantac as much as 50 percent higher than Tagamet. Glaxo then reinvested the revenue from early sales of Zantac into an extensive and comprehensive marketing campaign. Moreover, Glaxo marketed Zantac for both ulcers and heartburn, expanding the potential market. As a result, Zantac outsold Tagamet in the year preceding 1987, and earned Glaxo $2 billion.

The author notes several lessons to be learned from the ulcer blockbuster narrative. Firstly, "although science and scientific approach are important for drug discovery, close and regular collaboration between chemists and biologists is essential." In other words, the pharmaceutical industry can work more efficiently when the chemists and biologists work close together to avoid frivolous work.

Secondly, a balance must exist between patent protection and complete openness with the scientific community. Here, Black published and lectured extensively on the mechanisms and theories behind Tagamet. The downside was Glaxo could seize on the research and develop Zantac. The upside from this openness was because the technology behind Tagamet was so new, many in the scientific community offered opinions, critiques, and advice, which in turn resulted in "almost unlimited resources in elucidating the unique mechanisms."

C. Antihistamines

Allergies are the sixth most common cause of illness in the US. Allergens invoke the body's immune system and T-cells in the blood and tissues to produce substances that control the production of immunoglobulin E, a class of antibodies. The body then over produces immunoglobulins and attach to the receptors on the surface of mast cells, releasing histamines, leukotrienes and other inflammatory molecules causing swelling, itching, redness, skin eruptions, sneezing, runny noses, and watery eyes. Antihistamines relieve allergy symptoms by attaching to the histamine receptors, thereby blocking the signals that cause allergies.

Many medications were used to attempt to alleviate allergy symptoms before the development of antihistamines, such as opiates, belladonna, or asthma cigarettes. However, Li argues none of the conventional treatments were as effective as antihistamines, and even some of the early antihistamines had their problems.

One of the first antihistamines discovered and widely used was Benadryl. Benadryl was discovered in 1940 by George Rieveschl and was successfully brought to market in 1946. However, the downside of Benadryl and the other early antihistamines was drowsiness. Therefore, pharmaceutical companies recognized the demand for an antihistamine that would not cause drowsiness.

Aventis Pharmaceutical's Seldane and Schering-Plough's Claritin dominated the second generation of antihistamines. When Seldane was introduced in 1995, it was the first antihistamine to not cause drowsiness because it barely crossed the user's blood brain barrier. Moreover, Seldane was the first drug to be advertised directly to consumers through commercials on television. As such, Seldane easily cornered the market and garnered $500 million. Li notes that although Seldane was not a blockbuster drug *per se*, as it did not reach the $1 billion mark, "the way it was marketed heralded the era of blockbuster drugs."

Claritin was introduced into the market in 1993 after years of unnecessary review by the FDA. To make up for the delayed introduction, Schering-Plough invested $322 million into Claritin's marketing campaign. Like Seldane, Claritin was marketed through commercials. However, the author notes the importance of the "FDA relax[ing] its rules for TV commercials for drugs" and allowing drug companies to tell consumers to "ask your doctor" for more information. The marketing campaign contributed to annual sales of $1.4 billion in 1997 and $2.6 billion by 2000.

D. Blood Thinners

Li identifies two blockbuster blood thinners, Heparin and Plavix. Jay McLean discovered Heparin in 1916. Heparin works by binding to the active site on the surface of the plasma protein antithrombin, converting the serine protease inhibitor into an anticoagulant. Even a century later, Heparin is still used in clinics and hospitals for hemodialysis and vascular surgery, despite poor media attention from a medical scandal in 2008 when tainted Heparin produced in China resulted in 149 deaths worldwide.

Jean-Pierre Maffrand discovered Plavix in 1975 in a Sanofi laboratory. However, it was not until 1997, after a partnership with BMS, did Sanofi file a New Drug Application (NDA) with the FDA. Plavix was granted a Priority Review, an honor given only to the most important new drugs and was granted market approval by November 1997. By 1998, 3 million Americans were taking Plavix. In 2006 however, Plavix became embroiled in a patent dispute.

The roots of Plavix's patent dispute arose in market exclusivity and patent protection. Traditionally generic drug makers wait until the patent or market exclusivity of a drug expires before entering the market. However, because of the lucrative profits of blockbusters, many generic drug makers want to begin selling a generic version of a blockbuster early, and therefore challenge the legality of the patents on blockbuster drugs. Moreover, if a generic drug manufacturer is successful in patent litigation, they

are awarded a six month period of market exclusivity to sell their generic version. Patent litigation for blockbusters is potentially worth billions of dollars.

The patent litigation began when Apotex, a generic drug maker, challenged the validity of the Plavix patent in the European Union, Canada, and the US. Apotex's complaint that stated the Plavix's 1989 patent, which covered Plavix's right handed isomer, was already covered by another patent issued to Sanofi in 1985. Sanofi countersued for infringement on the Plavix patent. The litigation shook the confidence of investors and the two parties attempted to settle out of court. However, the Federal Trade Commission (FTC) regulates such settlements, and decided to deny the settlement. The parties tried to settle again and developed a new agreement, whereby Apotex would not launch its generic Plavix until eight months before the normal patent expiration. In return, Sanofi would pay Apotex $40 million. However, both parties agreed if the FTC rejected the settlement again, then Apotex would be allowed to distribute the generic drug immediately.

The FTC rejected the agreement and Apotex immediately began selling the generic Plavix. However, a federal judge ordered the shipments and sales halted immediately. A full trial was held, and the court found for Sanofi. The court held Apotex had failed to prove with clear and convincing evidence the patent was invalid. Damages were calculated at $442 million.

E. Pain Management

Li argues that for millennia, mankind struggled to overcome pain. Many techniques were developed overtime, ranging from acupuncture in China, to hypnosis in France. Even today, Li identifies pain as the "number one reason for Americans to visit a physician."

Pain is caused when several endogenous substances (histamine, serotonin, pro-

ton, bradykinin, and prostaglandins E2 and I2) are injected into tissue. The most common drugs used to treat pain are non-steroidal anti-inflammatory drugs [NSAID], with Aspirin being the first and most famous. Aspirin was the most commercially successful drug according to the *Guinness Book of World Records*. However, Aspirin's mechanism to prevent pain was not understood until the 1970s when John Vane discovered that Aspirin blocks the function of cyclooxygenase, which in turn blocks the production of prostaglandins E2 and I2. In other words, Aspirin forms a covalent bond with the cyclooxygenase enzyme and inhibits its activity, thus preventing pain.

The more modern and most successful NSAIDs are Celebrex and the other COX-2 inhibitors. During the 1980s, researchers discovered and examined two subtypes of cyclooxygenase. These two subtypes were named COX-1 and COX-2 respectively. COX-1 is responsible for normal physiological processes. COX-2 is in inflammatory cells and tissues and activates during an inflammatory response. Therefore, by inhibiting COX-2, a drug can stop prostaglandin production (one of the endogenous substances listed above), thus preventing pain.

The most famous and successful COX-2 inhibitor is Celebrex. Monsanto first developed Celebrex in 1993. However, Pharmacia acquired Monsanto's pharmaceutical division and therefore Celebrex in 1998. Pharmacia, along with Pfizer, began marketing Celebrex in 1999 and it immediately became a blockbuster drug and promised enormous profits to Pharmacia. Pfizer, however, recognized both the incredible financial potential of Celebrex, and the COX-2 process, and therefore acquired Pharmacia, thus securing exclusive rights, to Celebrex.

Li identifies pregabalin, specifically Lyrica, as another highly successful class of pain killers. Richard Silverman at Northwestern University first began the development of pregabalin with his synthesis of the 3-alkyl-GABA compounds in 1988. After Silverman filed a patent, the Northwestern University Technology Transfer Office

then reached out to pharmaceutical companies to further test Silverman's compounds. Parke-Davis agreed.

Parke-Davis discovered that (S)-2-isobutyl-GABA, the compound that later became Lyrica, was the most potent anticonvulsant agent they had ever tested. Parke-Davis in 1995 filed an investigational new drug (IND) application with the FDA and began Phase I clinical trials. During these trials, it was discovered that Lyrica effectively treated both pain and anxiety. In 2000, Parke-Davis was taken over by Pfizer. Pfizer continued the Phase 1 trials for Lyrica and in 2003 filed an NDA with the FDA which was later approved.

Pfizer continued to test, apply for, and receive additional drug indications for Lyrica, including indications for the treatment of seizures, fibromyalgia and epilepsy. As a result, by 2010, Lyrica was earning Pfizer $3 billion a year. Moreover, Lyrica also provided enormous financial success to both Northwestern University and Silverman. In 2007, Northwestern University after collecting approximately $70 million in royalties sold its stake in Lyrica for $700 million. Silverman himself donated money to Northwestern University in order to build a new science building.

V. How to Sustain the Blockbuster Drug Model?

The author argues that the current patent and the compensation systems governing the pharmaceutical industry need reform. Li argues the 20 year patent life for new drugs is insufficient for the drug maker to recover enough money to cover the development and marketing costs for new drugs. Specifically, Li finds the research and development of new drugs has changed drastically over the past decades. Firstly, the "easy" drugs curing mass problems are discovered and marketed, therefore it is harder to develop a novel drug to bring to market successfully. Secondly, the FDA's standard of review for new drugs is high. The higher the standard of review, the more intensive the clinical trials must be, and the more intensive a clinical trial is, the more expensive it becomes. In

other words, the high standards of review cost pharmaceutical companies more money to fully bring an idea to market. The author points out it takes $1.3 billion to take a drug from an idea to market. Therefore, innovation decreases as many small drug developers simply cannot afford the high costs of passing the FDA's review process.

The compensation system for the inventors of new drugs is in dire need for reform as well. For example, Bruce Roth, the inventor of Lipitor, was given a meager compensation compared to the billions of dollars generated for Parke-Davis. The rationale for such low relative compensation and low retirement packages is that "they were unlikely to discover more blockbuster drugs after their initial successful discoveries."

VI. Conclusion

The blockbuster business model has served the pharmaceutical industry and the public well for decades: patients had access to affordable, effective drugs, and drug makers reaped large profits. Li extensively examined the four major therapeutic areas and explained the history, chemistry, business methods, and people that made each identified blockbuster successful. This analysis is however, reflective.

Today, Li identifies present and future problems of the blockbuster business model. Firstly, many of the patents protecting the blockbuster drugs expired and with them the market exclusivity which largely contributed to large profit margins. Secondly, the "low hanging" blockbusters have been plucked, and therefore fewer blockbusters have come to market in recent years. As result, there are few new blockbusters to replace the lost revenue streams of the expired blockbusters. These two phenomena resulted in many rash decisions, such as mergers. For example, Pfizer either merged with or bought three separate rival pharmaceutical companies. The result of these mergers is less competition and innovation in drug development. Moreover, another result is large pharmaceutical companies outsourcing work to Contract Research Organizations (CROs) in China and India, at the cost of the US CROs.

These problems are characteristic of the small-molecule blockbuster drug, which comprised more than 90% of the last century's blockbusters. The author pins his hopes on the emergence of blockbuster biologic drugs to replace the small-molecule blockbuster.