SYRACUSE JOURNAL OF SCIENCE & TECHNOLOGY LAW

VOLUME 31 2014-2015

TABLE OF CONTENTS

SYRACUSE JOURNAL OF SCIENCE & TECHNOLOGY LAW

VOLUME 31 2014-2015

2014-2015 EDITORIAL STAFF

SYRACUSE JOURNAL OF SCIENCE & TECHNOLOGY LAW

VOLUME 31 2014-2015 ARTICLE 1, PAGE 1

HOW MUCH DOES J. CREW REALLY KNOW ABOUT YOU?: THE HARSH REALITY OF A MEGA-RETAILER'S PRIVACY POLICY

Laura Fleming

ABSTRACT

This paper seeks to illustrate what a typical privacy policy of a mass retailer looks like, as very few people actually bother to read a website's privacy policy. Also, accompanying each section of the privacy policy, this note will discuss the consequences each section has on consumers, as well as solutions for better protecting privacy. The second half of this paper will focus on the different methods available to consumers for enforcing their privacy rights. Furthermore, we will we look at a bill, which, while it ultimately did not pass, offered good solutions for best protecting consumer privacy. While this bill was not successful, it will undoubtedly help provide the framework for future privacy laws. Finally, this note will discuss measures that consumers, who wish to protect their personal information from retailers, can take, until Congress enacts suitable privacy laws.

INTRODUCTION

Nowadays, one cannot visit an online shopping website which does not display a privacy policy. A privacy policy is a statement that declares a website's policy on the collection and release of information about a visitor.[1] Privacy policies usually state what specific information the company collects and whether this information is kept confidential, shared, or sold to third parties.[2] However, very few people actually take the time to read through the privacy policy and consider its implications.[3] While most retailers provide links to its privacy policy, and most companies send an email to subscribers when the company updates the policy, the link is usually in small font at the bottom of the page; thus, many website visitors never even notice that the policy is available for viewing.

Despite the growing number of online retailers, there are very few laws regulating companies' use of customers' personal information.[4] Most states, with the exception of California, do not require retailers to provide privacy policies.[5] However, while state law may not require a retailer to post a privacy policy, federal law might.[6] For example, by the Children's Online Privacy Protection Act (COPPA), websites that collect personal information from

---

[1] BUS. DICTIONARY, http://www.businessdictionary.com/definition/privacy-policy.html (last visited Feb. 16, 2014).

[2] *Id.*

[3] Shankar Vedantam, *To Read All Those Web Privacy Policies, Just Take A Month Off Work*, NAT'L PUB. RADIO (Apr. 19, 2012, 3:30 AM), http://www.npr.org/blogs/alltechconsidered/2012/04/19/150905465/to-read-all-those-web-privacy-policies-just-take-a-month-off-work.

[4] Robert V. Connelly Jr., *Are Online Privacy Policies Required By Law?*, THE RVC BLOG (Oct. 25, 2010), http://www.rendervisionsconsulting.com/blog/are-online-privacy-policies-required-by-law/#sthash.i0K1u5fv.dpuf.

[5] *Id.*

[6] *Id.*

children under the age of thirteen must provide a privacy policy.[7] Nevertheless, this widespread lack of regulation leads to a lack of privacy, which this society values highly.

Accordingly, this paper will step through the privacy policy of one of America's largest online retailers, J.Crew, and explain the implications of each section on the customer. J.Crew's online store brought in over $134 million in revenue in 2012 and offers online shopping in 107 countries.[8] In addition, J.Crew's website rated the strongest for customer service speed and quality.[9] This adds to J.Crew's already great online reputation and draws even more customers to its online shop.

Furthermore, this paper will examine the options available to consumers who are concerned for their privacy, due to the ever-expanding collection of personal information by retailers. Then, this paper will discuss a recent bill, which attempted to protect consumers by implementing consumer-friendly policies regarding privacy policies. Finally, this paper will identify precautions and steps customers can take to protect their personal information from being used to their disadvantage by retailers seeking to cash in.

---

[7] *Children's Privacy*, BUREAU OF CONSUMER PROT. BUS. CTR., http://www.business.ftc.gov/privacy-and-security/children%27s-privacy (last visited Feb. 16, 2014).

[8] Lydia Dishnman, *Inside J. Crew's Move Back to Black*, FORBES (AUG. 30, 2012, 4:22 PM), http://www.forbes.com/sites/lydiadishman/ 2012/08/30/inside-j-crews-move-back-to-black/; Stephen Cotterill, *'Hello, World,' J.Crew says, via the web*, INTERNET RETAILER (June 27, 2014, 2:34 PM), http://www.internetretailer.com/2012/06/27/hello-world-jcrew-says-web.

[9] Lorna Pappas, *J.Crew, L.L. Bean And Net-A-Porter Among Best Online Customer Serv. Providers*, RETAIL TOUCHPOINTS (Sept. 11, 2013), http://www.retailtouchpoints.com/in-store-insights/2871-jcrew-ll-bean-and-net-a-porter-among-best-online-customer-service-providers.

I. ANALYSIS OF J.CREW'S PRIVACY POLICY

A. Collection Of Information

1. Information You Provide

The first section of J.Crew's privacy policy states that J.Crew collects information that customers provide.

> For example, [J.Crew] collect[s] information when you use [its] websites, shop in [J.Crew's] stores, call [J.Crew] on the phone, create an online account, sign up to receive…emails, request a catalog, participate in a sweepstakes, contest, promotion or survey, communicate with [J.Crew] via third party social media sites, request customer support, apply for a job or otherwise communicate with [J.Crew]. The types of information [J.Crew] may collect include your name, email address, zip code, billing address, shipping address, phone number, payment card information, product preferences, demographic information and any other information you choose to provide. In some cases, [J.Crew] may also collect information you provide about others, such as when you purchase a gift card for someone…, create and share a "wish list" or decide to purchase and ship products to someone. [J.Crew] will use this information to fulfill your requests and will not send marketing communications to your contacts unless they separately opt in to receive communications from [J.Crew].[10]

While consumers are most likely aware of the ramifications of providing information, such as a phone number or email address, there is one piece of information that may seem harmless to provide, but which, in fact, is not harmless. This unlikely source of personal information is the customer's ZIP code.[11] When a customer provides a retailer with this five-digit number, the customer opens the door to an abundance of junk mail and telemarketing calls.[12] As a result, Paul Stephens, the director of policy and advocacy for Privacy Rights Clearinghouse, a nonprofit watchdog group based in San Diego, California, recommends saying "no" when asked

---

[10] *Privacy Policy*, J.CREW, https://www.jcrew.com/help/privacy_policy.jsp (last visited Feb. 16, 2014) [hereinafter J.CREW).

[11] A. Pawlowski, *Should You Tell Stores Your ZIP code? Privacy Advocates Say No*, CNBC (Mar. 19, 2013, 2:14 PM), http://www.cnbc.com/id/100569424.

[12] *Id.*

for your ZIP code by a retailer.[13] This is because when a retailer pairs your ZIP code with your name, it can determine your mailing address, phone number, and specific demographic information.[14] Therefore, while a customer may believe they are only providing their ZIP code to the retailer, they are actually providing the company with much more personal information.

Accordingly, retailers are able to transform a ZIP code into valuable personal information through direct marketing services companies, such as Harte-Hanks, which offers the GeoCapture service to retailers.[15] Therefore, once the retailer obtains the customer's name from running their credit card and obtains the customer's ZIP code, this service "matches the collected information to a comprehensive consumer database to return an address."[16] Now armed with customer addresses, retailers can send mail marketing directly to customers.[17]

In response to these services, Massachusetts and California declared this practice violates their privacy laws.[18] These states ruled that a ZIP code amounts to "personal identification information."[19] However, while a customer can refuse to give their ZIP code while shopping in-

[13] *Id.*

[14] *Id.*

[15] Adam Tanner, *Never Give Stores Your ZIP Code. Here's Why*, FORBES (June, 19, 2013, 8:19 AM), http://www.forbes.com/sites/ adamtanner/2013/06/19/theres-a-billion-reasons-not-to-give-stores-your-zip-code-ever/.

[16] *Id.*

[17] *Id.*

[18] Pawlowski, *supra* note 11.

[19] *Id.*

store, online it is much more difficult.[20] This is because you need to provide a ZIP code for your shipping and billing addresses.[21]

However, there is an option for online shoppers who are required to provide their ZIP code in order to receive their package. A customer can opt out of most solicitations by registering with the Direct Marketing Association's Mail Preference Service.[22] Nevertheless, belonging to any database does open you up to the small risk that your information could be part of a wholesale data theft and ultimately used to steal your identity.[23]

Another valuable, yet more obvious, source of information for retailers is a customer's email address. For that reason, most retailers display a box on its homepage where patrons can sign up to receive emails from the company.[24] However, once a user enters their email address, most companies redirect the customer to a form where the company requests even more information.[25] Further requested information typically includes address, gender, preferred store, date of birth, and ZIP code.[26] As for J.Crew, this retailer offers an email sign-up box at the bottom right hand side of its webpage, and once one enters their email address they are redirected to a screen that asks for their first and last name, ZIP code, and country.[27] Therefore,

---

[20] *Id.*

[21] *Id.*

[22] Marlys Harris, *Asking for Your ZIP Code: A New No-No for Retailers?*, CBS MONEY WATCH (Feb. 17, 2011, 5:24 PM), http://www.cbsnews.com/8301-505145_162-38140938/.

[23] *Id.*

[24] David Moth, *Email sign up forms: a look at how 16 fashion retailers collect customer data*, ECONSULTANCY (July, 24, 2013), http://econsultancy.com/us/blog/63124-email-sign-up-forms-a-look-at-how-16-fashion-retailers-collect-customer-data.

[25] *Id.*

[26] *Id.*

[27] *See* J.CREW, *supra* note 10.

by obtaining a customer's name and ZIP code, J.Crew can send this information to direct marketing service companies to obtain even more personal information about the customer.

2. Information the Retailer Collects Automatically

The second section of J.Crew's privacy policy relates to information the company collects automatically whenever a customer visits its website or transacts business with the company.[28] The policy states that J.Crew collects information about:

> your use of [its] websites, such as the type of browser you use, access times, pages viewed, your IP address and the referring link through which you accessed [J.Crew's] websites…[Also,] [w]hen you purchase or return a product, [J.Crew] collect[s] information about the transaction, such as product details and the date and location of the purchase/return…[Additionally, J.Crew] may use cookies…and other tracking technologies to collect information about you when you interact with [J.Crew's] websites…, including information about your browsing and purchasing behavior. [J.Crew] may combine this information with other information [it] collect[s] about you and use it for various purposes, such as improving [its] websites and your online experience, understanding which areas and features of [its] sites are popular, counting visits, understanding campaign effectiveness, tailoring [its] communications with you, determining whether an email has been opened and links within the email have been clicked and for other internal business purposes.[29]

For this section of J.Crew's privacy policy, this paper will focus on retailers' use of customer return information, browser cookies, cell-phones, and IP addresses for collecting customer information.

While most people are aware that a retailer requests a customer's email address at the register or online with intent to keep the customer informed of promotions and track their purchase history from the company, most customers are not aware that information tracking

---

[28] *Id.*

[29] *Id.*

customer returns is just as important for retailers.[30] Nonetheless, since consumers return about $264 billion worth of merchandise each year, which is equivalent to almost 9% of total sales, retailers want to be able to identify chronic returners or gangs of thieves trying to make off with high-end products that are returned later for store credit.[31]

Thus, when one goes to make a return at a store, most retailers ask to see the customer's driver's license.[32] Typically, the information taken from a customer's license includes the identification number, the customer's name, address, date of birth, and expiration date.[33] This is because retailers collect customer return information and outsource that information to third parties, such as The Retail Equation, which create "return profiles" of customers.[34] These "return profiles" catalog and analyze the customer's returns at the store and online.[35] While customers consider this practice an invasion of privacy, the retail industry defends its practices, "claiming that this method is used to fight theft, not monitor its shoppers."[36] Bob Schoshinski, Assistant Director of the Federal Trade Commission's Division of Privacy and Identity Protection, stated that "[m]ost people think when they hand over a driver's license that it's just to confirm identity and not to be kept to be used for future transactions;" however, "[i]t shouldn't be that a third

[30] Jennifer C. Kerr, *Retailers keeping tabs on consumers' return habits*, YAHOO! FINANCE (Aug. 12, 2013, 3:27 PM), http://finance.yahoo.com/news/retailers-keeping-tabs-consumers-return-115934658.html.

[31] *Id.*

[32] *Id.*

[33] *Id.*

[34] *Id.*

[35] Kerr, *supra* note 30.

[36] *Id.*

party is keeping a profile on someone without them being informed what's going to happen when they hand over their driver's license or some other information to a retailer."[37]

Consequently, once the retailer receives a customer's "return profile," if there is a pattern of questionable returns, which suggests possible fraud, the retailer could then deny returns by that shopper at the store for a certain period of time, determined by the retailer.[38] The Retail Equation claims, however, that once the company analyzes consumer information, it only reports back to the specific retailer that requested the information, not all retailers that use the service.[39]

Nevertheless, consumers are not happy with this information sharing technique. However, lawsuits in this area have been ineffective.[40] In 2011, a man filed a lawsuit against Best Buy after the store swiped his driver's license for a return.[41] The man requested that the manager delete the information, to which he refused.[42] Thus, the plaintiff alleged that Best Buy violated privacy law when it swiped the license. However, a federal appeals court held that the Driver's Privacy Protection Act did not apply in these circumstances.[43]

As for tracking technologies, one common type of tracking used by retailers is "browser cookies." Browser cookies are text files that gather information about a computer user's Internet habits.[44] Browser cookies "contain unique identifiers and associate 'browsing history

---

[37] *Id.*

[38] *Id.*

[39] *Id.*

[40] Kerr, *supra* note 30.

[41] *Id.*

[42] *Id.*

[43] *Id.*

[44] Bose v. Interclick, Inc., No. 10 Civ. 9183(DAB), 2011 WL 4343517, at *1 (S.D.N.Y. Aug. 17, 2011).

information' with particular computers."[45] Advertising networks use this browsing history information to create "behavioral profiles."[46] Thus, when a computer user visits a web page, on which the advertising network provides advertisements, the advertising network uses a behavioral profile to select particular advertisements to display on that computer.[47]

Furthermore, if you've ever noticed an item you looked at online reappear in an ad on another website, this is because online retailers assign customers a virtual identification number and track customers as they go from site to site.[48] As a result, retailers "purchase targeted ads for products they already know you're strongly interested in."[49]

An explanation of the way this advertising occurs is as follows: First, commercial websites rent out online advertising "space" to other websites.[50] Then, in the simplest arrangement, the host website rents space on its web pages to another website, which allows the website to place a banner advertisement on the web page.[51] Next, when a user on the host website clicks on the banner advertisement, the user is automatically connected to the advertiser's website.[52] Thus, companies, such as DoubleClick, act as intermediaries between the host websites and websites seeking to advertise.[53] These companies promise retailers that they

---

[45] *Id.*

[46] *Id.*

[47] *Id.* at *1.

[48] Christopher Matthews, *Future of Retail: How Companies Can Employ Big Data to Create a Better Shopping Experience*, TIME (Aug. 31, 2012), *available at* http://business.time.com/2012/08/31/future-of-retail-how-companies-can-employ-big-data-to-create-a-better-shopping-experience/.

[49] *Id.*

[50] *In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 502 (S.D.N.Y. 2001).

[51] *Id.*

[52] *Id.*

[53] *Id.*

will "place their banner advertisements in front of viewers who match their demographic target."[54] This is possible because, when users visit any of these affiliated websites, a "cookie" is placed on their hard drives.[55] Afterward, the companies' cookies store this personal information on users' hard drives until it can electronically access the cookies and upload the data.[56] Once companies such as DoubleClick collect information from the cookies on users' hard drives, it compiles the information to build demographic profiles of users.[57] Then, DoubleClick and its licensees target banner advertisements using these demographic profiles.[58]

Consumers who are apprehensive about the practice of tracking "browser cookies" have two solutions. First, computer users can delete or block their "browser cookies," which prevents third parties from associating the user's browsing history information with their subsequent web activity.[59] Second, the computer user can visit the host website and request an "opt-out" cookie, which informs the website not to install third party advertiser cookies on the user's browser.[60]

Appropriately, there has been much litigation in this area under the Electronic Communications Privacy Act; however, this litigation has not been successful for consumers. As one court noted, "cookie[s]…are much akin to computer bar-codes or identification numbers

---

[54] *Id.*

[55] *DoubleClick,* 154 F.Supp. 2d at 502-03.

[56] *Id.* at 503.

[57] *Id.* at 505.

[58] *Id.* at 504-05.

[59] *Id.*

[60] *DoubleClick,* 154 F.Supp. 2d at 504; *Manage Cookies, What is an Opt Out Cookie?*, ALL ABOUT COOKIES, http://www.allaboutcookies.org/manage-cookies/opt-out-cookies.html (last visited Nov. 15, 2014).

placed on 'business reply cards' found in magazines."[61] While these bar-codes and identification numbers are "meaningless to consumers", they are "valuable to companies in compiling data on consumer responses."[62]

For example, in *In re DoubleClick*, a class action lawsuit was brought against DoubleClick, "the largest provider of Internet advertising products and services in the world," alleging violations of the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act, and state law claims of trespass and unjust enrichment.[63] There, the "[p]laintiffs allege[d] that DoubleClick's cookies collect[ed] 'information that Web users, including plaintiffs and the Class, consider to be personal and private.'"[64] This information included customer names, e-mail addresses, addresses, telephone numbers, searches performed on the Internet, websites visited on the Internet, and "information that users would not ordinarily expect advertisers to be able to collect."[65] However, the court found that DoubleClick's cookies only collected information regarding users activities on DoubleClick-affiliated Web sites.[66] Also, DoubleClick never accessed files, programs, or other information on users' hard drives.[67] Additionally, DoubleClick did not collect information from a user who took the steps to opt-out of DoubleClick's tracking.[68]

---

[61] *DoubleClick*, 154 F. Supp. 2d at 513.

[62] *Id.*

[63] *Id.* at 500, 513; 18 U.S.C. § 2701 (2002).

[64] *DoubleClick*, 154 F. Supp. 2d at 503.

[65] *Id.*

[66] *Id.* at 502-03.

[67] *Id.* at 504.

[68] *Id.* at 503.

Thus, in order for DoubleClick's actions to be considered unlawful access to stored communication by 18 U.S.C.A. §2701, the cookies long-term residence on users' hard drives must be considered "electronic storage."[69] Section 2510(17) defines "electronic storage" as: "(A) any *temporary, intermediate storage* of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication *by an electronic communication service* for the purpose of backup protection of such communication."[70] However, "the cookies' residence on plaintiffs' computers does not fall into § 2510(17)(B) because plaintiffs are not 'electronic communication service' providers."[71] Therefore, customers' cookies and identification numbers are not protected; thus, DoubleClick cannot be held liable for obtaining them.[72] In addition, the court found that the plaintiffs offered no proof to support their assertion that Doubleclick's access was unauthorized.[73] Instead, the facts alleged supported the position that DoubleClick-affiliated websites did authorize DoubleClick's access, since "the very reason clients hire DoubleClick is to target advertisements based on users' demographic profiles."[74] Therefore, the court dismissed the case with prejudice.[75]

Subsequently, in *Bose v. Interclick*, Bose alleged that Interclick used "flash cookies" (or Local Shared Objects ("LSOs")) to back up browser cookies.[76] According to the Computer Fraud

[69] *DoubleClick*, 154 F. Supp. 2d at 511.

[70] *Id.*

[71] *Id.*

[72] *Id.* at 513.

[73] *Id.* at 510.

[74] *DoubleClick*, 154 F. Supp. 2d at 510.

[75] *Id.* at 526.

[76] Bose v. Interclick, Inc., No. 10 Civ. 9183(DAB), 2011 WL 4343517, at *1 (S.D.N.Y. Aug. 17, 2011).

and Abuse Act (CFAA), "[w]hoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer ... shall be punished."[77] Under § 1030(a)(5)(C), the CFAA also subjects someone who "intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage," to criminal liability.[78] However, the court held that the collection of demographic information does not "constitute[ ] damage to consumers or unjust enrichment to collectors."[79] In addition, the court likened advertising on the Internet to advertising on television or in newspapers.[80] Thus, even if Bose took steps to prevent the data collection, the plaintiff's injury is still insufficient to meet the statutory threshold.[81]

Another type of tracking technology that is on the rise is the collection of customer information through their cell phones. When customers shop in-store, stores are collecting information about customer shopping habits "using video surveillance and signals from [consumers] cell phones and apps to learn information as varied as their sex, how many minutes they spend in the…aisle and how long they look at merchandise before buying it."[82] This tracking is possible through companies such as RetailNext, which collects data from shoppers' smart phones in order to track shopping patterns.[83] Therefore, if a shopper has the Wi-Fi on their

---

[77] 18 U.S.C. § 1030(a)(2)(C) (2008).

[78] 18 U.S.C. § 1030(a)(5)(C) (2008); *Bose*, 2011 WL 4343517, at *3.

[79] *Bose*, 2011 WL 4343517, at *3 (citing *DoubleClick*, 154 F. Supp. 2d at 525).

[80] *Id.*

[81] *DoubleClick*, 154 F. Supp. 2d at 497; *Bose*, 2011 WL 4343517, at *5.

[82] Stephanie Clifford & Quentin Hardy, *Attention, Shoppers: Store Is Tracking Your Cell*, N.Y. TIMES (July, 14, 2013), http://www.nytimes.com/2013/07/15/business/attention-shopper-stores-are-tracking-your-cell.html?pagewanted=all&_r=0.

[83] *Id.*

phone turned on, a store that offers Wi-Fi is able to place the shopper's location in the store, even if the shopper does not connect to the network.[84] However, the use of tracking on smart phones makes many people uncomfortable.[85] Nevertheless, marketing through smart phones is believed to be the next big thing for retailers.[86] This is because "smartphones can bridge the gap between the online and offline worlds…[as] users always have their phones with them, even when they're not browsing the Internet."[87] Thus, "[r]etailers can learn about a customer through their online shopping behavior and then offer them short-term discounts through a cell-phone when the consumer is near that store[']s brick-and-mortar location."[88]

Nevertheless, it all comes down to retailers attempting to get consumers to buy more. While brick-and-mortar stores once cringed at the thought of customers using their phones to compare prices at competitor stores, now retailers are creating and publicizing their own mobile apps and offering in-store Wi-Fi.[89] Through these mobile apps, retailers can provide shoppers with coupons as they move throughout the store.[90] Also, Wi-Fi enables retailers to track the potential customer's online movements, which can further help retailers tailor advertisements and promotions to the specific consumer.[91]

---

[84] *Id.*

[85] Matthews, *supra* note 48; Chris Moran, *4 Ways Retail Stores Are Monitoring Your Every Move*, CONSUMERIST (Mar. 27, 2013), http://consumerist.com/2013/03/27/4-ways-retail-stores-are-monitoring-your-every-move/.

[86] Matthews, *supra* note 48; Moran, *supra* note 85.

[87] *Id.*

[88] Moran, *supra* note 85.

[89] Associated Press, *Technology digs deeper into personal shopping habits*, DENVER POST (Nov. 29, 2013), *available at* http://www.denverpost.com/nationworld/ci_24621678/technology-digs-deeper-into-personal-shopping-habits#ixzz2rQkFXHKh (last visited Nov. 15, 2014) [hereinafter *Technology digs deeper*].

[90] *Id.*

[91] *Id.*

While consumers are less worried about websites tracking their cookies, "some bristle at the physical version, at a time when government surveillance — of telephone calls, Internet activity and Postal Service deliveries — is front and center because of the leaks by Edward J. Snowden."[92] However, most Americans are willing to let companies access their personal data when provided with an incentive, such as additional savings or better service.[93] Yet, in response to customer complaints about this invasion of privacy, some retailers halted their cell phone tracking due to bad publicity.[94] On the other hand, some retailers claim that data collected at the point-of-sale "provides sufficient information without sparking the debate over individual consumers' privacy."[95]

Finally, another common tracking technology used by retailers is the determination of a consumer's approximate location. This is possible because a consumer's IP address can identify his approximate location.[96] Also, if a consumer is using a wireless connection, Wi-Fi triangulation can determine a consumer's location by surveying nearby wireless networks.[97] Not surprisingly, there is much concern over the tracking of location information, because it can pose a substantial privacy risk.[98] For example, by being able to reveal your whereabouts at any given

[92] Clifford, *supra* note 82.

[93] Ann Meyer, *Some Retailers Pull Back on Personalized Data Collection*, RETAIL LEADER, http://www.retailleader.net/top-story-tech___logistics-some_retailers_pull_back_on_personalized_data_collection-2294.html (last visited Nov. 15, 2014).

[94] *Id.*

[95] *Id.*

[96] *Online Privacy: Using the Internet Safely*, PRIVACY RIGHTS CLEARINGHOUSE, https://www.privacyrights.org/online-privacy-using-internet-safely (last visited Nov. 15, 2014) [hereinafter *Online Privacy*].

[97] *Id.*

[98] *Id.*

time, it can be dangerous for individuals being stalked or domestic violence victims.[99] However, consumers can block their IP address through services such as Tor.[100] Also, consumers can use a Virtual Private Network (VPN), which replaces the IP address with one from the VPN provider.[101]

iii. Information Collected from Partners or Other Sources

This section authorizes J.Crew to obtain customer information from other sources and combine that information with information J.Crew collects about its customers.[102]

> For example, [J.Crew] collect[s] information from the U.S. Postal Service's national change of address database to verify and update mailing addresses. In addition, if you apply for a J.Crew credit card, [J.Crew] obtain[s] limited information about you from the partner that manages [its] co-brand credit card program.[103]

Therefore, J.Crew can discover what addresses to send catalogues or coupons to by matching customer names with the U.S. Post Offices' database. In addition, J.Crew can receive spending information and habits from the company that manages its store credit card. The purpose of this practice is to ensure customers are receiving promotions and communications, thus making them more likely to make a purchase.

---

[99] *Id.*

[100] *Id.*

[101] *Online Privacy*, *supra* note 96.

[102] J.CREW, *supra* note 10.

[103] *Id.*

B. Use of Information

Once J.Crew collects information about its customers from the numerous sources discussed above, J.Crew uses that information for a variety of purposes.[104] J.Crew states that it uses customer information in order to:

> Facilitate and improve your in-store and online shopping experience; Provide the products and services you request, process transactions and send you related information, including confirmations and receipts; Respond to your comments, questions and requests and provide customer service; Communicate with you about products, services, offers, promotions, rewards and events and provide news and information we think will be of interest to you…; Manage your online account(s) and send you technical notices, updates, security alerts and support and administrative messages; Personalize your online experience and provide advertisements, content or features that match your profile and interests; Monitor and analyze trends, usage and activities; Process and deliver contest, promotion and sweepstakes entries and rewards; Link or combine with information we get from others to help understand your needs and provide you with better service; and [c]arry out any other purpose for which the information was collected.[105]

This section of the policy also states that customers "consent to the processing and transfer of information in and to the U.S. and other countries" when one accesses J.Crew's website or provides the company with personal information.[106]

There are two main types of practices that retailers use to track customer behavior through the methods discussed above. The first is "behavioral targeting."[107] Behavioral targeting is "the practice of collecting and compiling a record of individuals' online activities, interests, preferences, and/or communications over time."[108] Using the methods already discussed, such as cookies, retailers are able to "monitor individuals, the searches they make, the pages they visit,

---

[104] *Id.*

[105] *Id.*

[106] *Id.*

[107] *Online Privacy*, *supra* note 96.

[108] *Id.*

the content they view, their interactions on social networking sites, and the products and services they purchase."[109] Then, retailers use this information to display advertisements to a customer, based on their behavioral record.[110] These advertisements are "based upon an individual's web-browsing behavior, such as the pages they have visited or the searches they have made."[111] Behavioral targeting is growing and replacing "contextual marketing," which is when retailers target users with advertisements that are based only upon the given webpage's content.[112]

The second type of tracking used by retailers is known as "dynamic pricing."[113] Dynamic pricing is when a retailer charges "different prices to different consumers for identical goods or services."[114] This is also possible through the use of cookies.[115] Retailers are able to read the cookies on a customer's browser to determine what products a consumer searched for and bought and how much the consumer paid.[116] Using this information, the retailer predicts how much a customer might be willing to spend on a product.[117] Also, some retailers consider other factors when determining pricing.[118] For example, retailers may charge inflated prices to customers who

---

[109] *Id.*

[110] *Id.*

[111] *Id.*

[112] *Online Privacy*, *supra* note 96.

[113] *Online Shopping Tips: E-Commerce and You*, PRIVACY RIGHTS CLEARINGHOUSE, https://www.privacyrights.org/online-privacy-using-internet-safely (last visited Nov. 15, 2014) [hereinafter *Online Shopping Tips*].

[114] *Id.*

[115] *Id.*

[116] *Id.*

[117] *Id.*

[118] *Online Shopping Tips*, *supra* note 113.

make repeated returns.[119] This price adjusting is legal as long as determination of the prices is not made based on race, religion, or gender.[120]

However, there are multiple strategies a consumer can use to defeat both "behavioral targeting" and "dynamic pricing." Consumers can combat behavioral targeting through the methods discussed above, such as deleting cookies and opting out. As for dynamic pricing, first, customers should not log into a site before obtaining a price quote.[121] Also, by clearing the cookies from your browser before you visit a site, retailers will not be able to match up your past browsing history.[122] In addition, by visiting sites from different browsers, consumers can see if the prices are the same across the board.[123] Finally, by using price comparison sites, which check prices from multiple vendors, consumers can see if they are being offered an inflated price on one website.[124] Undoubtedly, the main purpose of either practice is to sell more products.

C. The Sharing of Your Information

The third section of J.Crew's privacy policy outlines the situations in which the company may share information about its customers.[125] This section states that J.Crew can share customer information with:

---

[119] *Id.*

[120] Khadeeja Safdar, *Online Retailers Track Consumer Spending Habits To Get Wealthier Customers To Spend More*, THE HUFFINGTON POST (July, 25, 2012, 5:26 PM), http://www.huffingtonpost.com/2012/06/29/online-retailers-track-spending-habits_n_1637679.html.

[121] *Online Shopping Tips*, *supra* note 113.

[122] *Id.*

[123] *Id.*

[124] *Id.*

[125] J.CREW, *supra* note 10.

> vendors, consultants and *other service providers* who need access to such information to carry out work on [J.Crew's] behalf;…[J.Crew's] business partners and other third parties for purposes of sending their own direct mail, *unless you opt out of this type of sharing by logging into your online account and changing your preferences* or by contacting [J.Crew]; In response to a request for information if [J.Crew] believe[s] disclosure is in accordance with any applicable law, regulation or legal process, or as otherwise required by any applicable law, rule or regulation; If [J.Crew] believe[s] your actions are inconsistent with [its] user agreements or policies, or to protect the rights, property and safety of [J.Crew] or any third party; In connection with, or during negotiations of, any merger, sale of company assets, financing or transfer of all or a portion of [J.Crew's] business to another company; and [w]ith your consent or at your direction. [J.Crew] may also share aggregated or de-identified information, which cannot reasonably be used to identify you (emphasis added).[126]

This section of the privacy policy authorizes J.Crew to share customer information with third parties. This includes the third party that J.Crew contracts out to in order to place advertisements on other websites of products previously viewed on J.Crew's website.[127] For example, one of these companies, Acerno, has 140 million people in the United States on file in its database.[128] This company tracks what Internet users buy and view and then uses this information to place advertisements on more than 400 websites on behalf of retailers.[129] Like the companies described earlier, Acerno builds files linked to an identification number and places cookies on the browsers of Internet users who visit websites within its network.[130] However, Acerno requires online retailers that use its service to disclose its practices in its privacy

---

[126] *Id.*

[127] *Id.*

[128] Saul Hansell, *What Online Stores Sell: Data About You*, N.Y. TIMES (Oct. 24, 2008, 8:53 AM), http://bits.blogs.nytimes.com/2008/10/24/what-online-stores-sell-data-about-you/?_r=0 (last visited Nov. 15, 2014).

[129] *Id.*

[130] *Id.*

policy.[131] Also, Acerno requires its retailer customers to provide users the option to not have their shopping data tracked.[132]

This section also covers the sharing of consumer information with an analytics firm that "digest[s] and analyze[s] all the 'big data' that retailers and others collect."[133] While some retailers, such as Nordstrom, invest in internal data analysis, most use the software provided by large analytic firms.[134] Retailers input customer information into this software in order to adjust its marketing to meet consumer demand and better understand what products to place on clearance.[135] This is possible because the software considers factors such as inventory counts, customer views, and items viewed but not ordered, among others.[136]

In addition, companies in the same line of business are increasingly sharing information between one another.[137] This type of data sharing is valuable to companies because "by scaling the information base to include a much more comprehensive dataset of customers as well as non-customers' behavior…resources could be created and accessed which are impossible to generate internally."[138] Accordingly, these "comprehensive datasets" are seen as "proprietary and a source

---

[131] *Id.*

[132] *Id.*

[133] Mohana Ravindranath, *Brooks Brothers, national retailers analyze 'big data' from sales to adjust marketing*, WASH. POST (Sept. 22, 2013), *available at* http://articles.washingtonpost.com/2013-09-22/business/42299416_1_brooks-brothers-analytics-sales-data.

[134] *Id.*

[135] *Id.*

[136] *Id.*

[137] John Tengberg, *Inter-Organizational Information Sharing of Customer Data in Retail* (May 2013) (Composite Info. Sys. Lab., Working Paper No. 2013-09), *available at* http://web.mit.edu/smadnick/www/wp/2013-09.pdf.

[138] *Id.* at 14.

of competitive advantage."[139] However, this type of data sharing could have unfortunate effects on consumers. This is because the more databases a consumer's information is in, the greater the probability this information could be stolen.

D. Advertising, Security, and Children

The next three sections of J.Crew's privacy policy deal with advertising, analytics services, security, and children.[140] First, J.Crew expressly states that the company engages third parties to serve advertisements on its behalf.[141] J.Crew clearly provides that the third parties (i.e. companies such as Ascerno) may use cookies, IP addresses, pages viewed, and links clicked in order to collect information about J.Crew's customers.[142] Then, J.Crew expressly claims that this information will be used to deliver advertising targeted to a customer's interests on not only J.Crew's website, but other websites as well.[143] Also, just as Ascerno requires, J.Crew offers the option to consumers of opting out of Internet-based ads or opting out of having web-browsing information used for behavioral advertising purposes.[144] J.Crew then links Network Advertising's website so customers can easily opt-out of tracking.[145]

---

[139] *Id.*

[140] J.CREW, *supra* note 10.

[141] *Id.*

[142] *Id.*

[143] *Id.* (After being on J.Crew's website for purposes of this paper, advertisements showed up on multiple websites I visited thereafter, including my personal email account.)

[144] *Id.*

[145] J.CREW, *supra* note 10.

Second, J.Crew states that it will take "reasonable measures" to protect consumer information from theft, misuse, and unauthorized access.[146] However, the policy does not state what J.Crew considers a "reasonable measure."

Lastly, J.Crew states that it does not collect personal information from children under the age of thirteen.[147] This is consistent with federal law governing information collection of children.[148]

E. Consumer Choices

The final section of J.Crew's privacy policy deals with the choices available to consumers pertaining to online account information, promotional communications, cookies, and California privacy rights.[149] The part dealing with online account information states that,

> [y]ou may update, correct or delete your online account information at any time by logging into your account and navigating to the "My Account" page or by contacting [J.Crew]. You can also contact [J.Crew] if you wish to deactivate your online account, but note that [J.Crew] may retain certain information as required by law or for legitimate business purposes. [J.Crew] may also retain cached or archived copies of information about you for a certain period of time.[150]

Thus, this section about online account information offers consumers the option of deleting their online account with J.Crew. However, J.Crew states that it may still keep information about its customers, even after they delete their online account. Suspiciously, J.Crew does not state how long it will keep this information about its customers or for what purpose

---

[146] *Id.*

[147] *Id.*

[148] *Children's Privacy*, *supra* note 7.

[149] J.CREW, *supra* note 10.

[150] *Id.*

J.Crew will use this information, other than generic "business purposes." Also, this section does not affect the information that J.Crew gathered from the customer's in-store shopping; therefore, J.Crew may still have and may still use personal information, such as the customer's name and ZIP code.

Next, the section of J.Crew's privacy policy pertaining to promotional communications states that customers can

> opt out of receiving promotional communications from [J.Crew] at any time…To opt out of direct mail (such as catalogs and post cards): Log into your online account and adjust your settings under the "Catalog Preferences" page or contact [J.Crew]. To opt out of promotional emails and text messages: Follow the instructions provided in those communications or contact [J.Crew]. Please note that even if you opt out of receiving promotional communications, [J.Crew] may continue to send you non-promotional emails, such as those about your account or [J.Crew's] ongoing business relations.[151]

Thus, this section about promotional communications offers consumers the option of opting out of email and direct mail correspondence with J.Crew. However, like the previous section, J.Crew states that it may still keep information about its customers, even after they opt-out of receiving communications. Also, J.Crew still retains the right to send customers, who opt-out of promotions, emails about their account for ambiguous "ongoing business relations." The vague "catch-all" provisions in this section and the previous section demonstrate the need for more transparency in privacy policies and the necessity for laws that require this transparency.

Furthermore, the privacy policy also states that customers can set their browsers to

> remove or reject cookies, but note that doing so does not necessarily affect third party flash cookies used in connection with [J.Crew's] websites. For more information about disabling flash cookies, see www.adobe.com/products/flashplayer/security. Please note that if you choose to remove or reject cookies, this could affect the availability and functionality of [J.Crew's] websites…If you enable Do Not Track, J.Crew will not use information about your web viewing activities to tailor your online experience on other websites operated by J.Crew…[H]owever,…[J.Crew's] third party advertising providers may continue to use information about your web viewing activities to tailor advertising to

[151] *Id.*

> your interests across different websites even when you have Do Not Track enabled in your browser.[152]

This section informs customers of the options available to them for preventing tracking, such as the methods discussed previously. However, J.Crew casts the choice of "opting out" of cookies in a bad light. By claiming that J.Crew cannot "tailor your online experience" if you opt out of cookies, J.Crew makes it seem as if customers are missing out on a custom online "experience." This is because J.Crew, and all retailers, gain major benefits, such as the one's discussed above, from tracking consumers' cookies.

Finally, under the section dealing with California privacy rights, the policy states that:

> residents of California…[may] request certain details about how their information is shared with third parties for direct marketing purposes. Under the law, a business must either provide this information or permit California residents to opt in to, or opt out of, this type of sharing. J.Crew permits California residents to opt out of having their information shared with third parties for direct marketing purposes. To opt out, please log into your online account and change your settings under the "Catalog Preferences" page or contact [J.Crew].[153]

This section exists because, currently, California is at the forefront of privacy policy laws benefiting consumers, which is hopefully a path other states will soon follow.[154]

II. THE NEED FOR PRIVACY POLICIES

In a time when privacy concerns are front and center, with recent headlines including the theft of mass numbers of customer information from Target and data leaks by Edward Snowden, the lack of laws dealing with privacy policies is concerning. With the exception of a couple states, most states do not have regulations governing privacy policies, and neither does federal

---

[152] *Id.*

[153] *Id.*

[154] Michelle Quinn, *California Driving Internet Policy*, POLITICO (Oct. 8, 2013, 5:06 AM), http://www.politico.com/story/2013/10/california-internet-privacy-policy-97964.html.

law, except in limited circumstances. In the United States, online privacy is based on a concept called "notice and choice."[155] This means that websites may gather and use consumer information, as long as consumers are informed and have the option to opt out of it.[156] However, there is a major problem with this system.[157] The problem is the fact that this system assumes that website users read the privacy policy, which is often not the case.[158]

A. Potential Lawsuits

As we have seen with J.Crew's privacy policy, privacy policies enable companies to collect all sorts of personal information about not only customers, but potential customers as well. Thus, simply by providing a privacy policy, retailers are authorized to track a consumer's every move online and in store. In response to the wide range of methods companies are using to collect consumer information, consumers, concerned for their privacy rights, have brought many lawsuits. As the cases previously discussed have shown, typically, lawsuits are brought under one or more of four categories. These categories include the Computer Fraud and Abuse Act, a state's consumer protection act, trespass to chattels, and unjust enrichment.[159]

First, under the Computer Fraud and Abuse Act, a claimant must prove that"[w]hoever knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains

---

[155] Hansell, *supra* note 128.

[156] *Id.*

[157] *Id.*

[158] *Id.*

[159] *See* Del Vecchio v. Amazon.com, Inc., C11-366RSL, 2012 WL 1997697 (W.D. Wash. June 1, 2012).

anything of value ... shall be punished."[160] While this is predominately a criminal statute, it also provides for a civil cause of action.[161] However, to succeed on a civil cause of action, the conduct must involve at least one of the following factors: "loss to 1 or more persons during any 1-year period aggregating at least $5,000 in value;" "the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;" "physical injury to any person;" "a threat to public health or safety;" "damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security;" or "damage affecting 10 or more protected computers during any 1-year period."[162] Nevertheless, it is usually difficult for a claimant to prove any one of these factors.[163] Arguably, the easiest factor to prove would be a loss of at least $5,000; however, the $5,000 cannot include "non-monetary detriments."[164] Accordingly, a court held that a claimant cannot argue that their private information has "economic value [equal to or] far in excess of $5,000," since their information was "economically exploitable" by the company.[165] Thus, the collection of private information alone is not enough to succeed under the Computer Fraud and Abuse Act.

Second, while states vary on what they require under their Consumer Protection Act, typically a claimant must prove "an unfair or deceptive act or practice,…injury to the plaintiff in

---

[160] *Del Vecchio*, 2012 WL 1997697 at *3; 18 U.S.C. § 1030(a)(4), (e)(2) (2008) (defining the term "protected computer" to include any computer "used in or affecting interstate or foreign commerce or communication").

[161] *Del Vecchio*, 2012 WL 1997697 at *3; 18 U.S.C. § 1030(g) (2008).

[162] *Id.*

[163] *Id.* at *4.

[164] *Id.*

[165] *Id.*

his or her business or property, and a causal link between the unfair or deceptive act and the injury suffered."[166] However, a claimant can allege an injury only if they can demonstrate that the company accessed the claimant's computer without authorization.[167] This is difficult to prove because typically the company's privacy policy notifies visitors of its actions (i.e. placing browser and Flash cookies on users' computers and using those cookies to collect information about the users' navigation and shopping habits).[168] Also, if the claimant made a purchase on the company's site, courts appear to conclude that action is sufficient acknowledgment "that cookies were being received and [there was] an implied acceptance of that fact."[169]

Third, under the tort theory of trespass to chattels, a party must prove intentional interference with the claimant's personal property, which deprives the owner of possession.[170] However, the one who intentionally interferes with the other's chattel is subject to liability only if "his intermeddling is harmful to the possessor's materially valuable interest in the physical condition, quality, or value of the chattel, or if the possessor is deprived of the use of the chattel for a substantial time, or some other legally protected interest of the possessor is affected…"[171]

[166] *Del Vecchio*, 2012 WL 1997697 at *6; *see* Gorbey ex rel. Maddox v. Am. Journal of Obstetrics & Gynecology, 849 F. Supp. 2d 162, 165 (D. Mass. 2012) (applying Massachusetts law); *see also* Goshen v. Mut. Life Ins. Co. of N.Y., 774 N.E. 2d 1190, 1193 (N.Y. 2002).

[167] *Del Vecchio*, 2012 WL 1997697 at *6.

[168] *Id.*

[169] *Id.*

[170] *Id.* at *8; *see* Sch. of Visual Arts v. Kuprewicz, 771 N.Y.S. 2d 804, 807 (N.Y. Sup. Ct. 2003).

[171] *Del Vecchio*, 2012 WL 1997697 at *8.

Therefore, plaintiffs may only prevail on this theory if the company sends thousands of requests to claimant's computer each day, or if the company's cookies bombard the claimant's computer with pop-up advertisements to the extent that viewing a webpage becomes impossible.[172]

Finally, under unjust enrichment, a claimant must prove that "(1) one party…conferred a benefit to the other; (2) the party receiving the benefit…[has] knowledge of that benefit; and (3) the party receiving the benefit…accept[ed] or retain[ed] the benefit under circumstances that make it inequitable for the receiving party to retain the benefit without paying its value."[173] Thus, "a person who is unjustly enriched *at the expense of another* is liable in restitution to the other."[174] However, courts have never considered the collection of demographic information, which is valuable for retailers, to constitute damage to the claimant or unjust enrichment to the collector.[175]

Nevertheless, while privacy policy lawsuits are mostly unsuccessful, most state and federal courts will hold a company to its privacy policy.[176] Therefore, if a company does something in contrast to its stated privacy policy, the company will likely be held accountable.[177] Also, many states have laws that hold companies liable for knowingly making a false or misleading statement in its privacy policy.[178] For example, in September of 2013, "users accused

---

[172] *Id.*

[173] *Id.* at *9; *see* Peterson v. Cellco P'ship, 80 Cal. Rptr. 3d 316, 323 (Cal. Ct. App. 2008); *see also* Mandarin Trading Ltd. v. Wildenstein, 944 N.E. 2d 1104, 1110 (N.Y. 2011).

[174] *Del Vecchio*, 2012 WL 1997697 at *9.

[175] *Id.*

[176] Robert V. Connelly Jr., *Are Online Privacy Policies Required By Law?*, THE RVC BLOG (Oct. 25, 2010), http://www.rendervisionsconsulting.com/blog/are-online-privacy-policies-required-by-law/#sthash.i0K1u5fv.dpuf.

[177] *Id.*

[178] *Id.*

Google of violating federal and state laws by intercepting people's emails in order to serve them ads that match keywords in messages."[179] Google defended its practices by claiming that users consented to email scanning when they accepted the company's terms of service.[180] However, Google's argument was unsuccessful on a summary judgment motion, because "Google didn't clearly explain to users that it might send ads based on email content."[181] This is because, even though Google "reserved the right to 'pre-screen' content," Google's privacy policy implied that content would be screened only to filter out objectionable material, not serve users targeted ads.[182] This ruling was said to reflect a "very consumer-friendly view of the privacy policy."[183]

Additionally, in December of 2013, users accused Apple of violating consumer protection laws by failing to follow its privacy policy.[184] However, the same judge that ruled on the Google lawsuit said, "consumers couldn't proceed without proof that they had read Apple's privacy policies."[185] This is troublesome because the law assumes that both parties to an agreement have read it.[186] Therefore, this ruling might indicate trouble for consumers who want to bring private lawsuits.[187]

---

[179] Wendy Davis, *Judge Rules Gmail Ads Might Violate Privacy*, MEDIAPOST (Sept. 26, 2013, 6:02 PM), http://www.mediapost.com/publications/article/210095/judge-rules-gmail-ads-might-violate-privacy.html.

[180] *Id.*

[181] *Id.*

[182] *Id.*

[183] *Id.*

[184] Wendy Davis, *Will Consumers' Loss Against Apple Affect Other Privacy Cases?*, MEDIAPOST (Dec. 5, 2013, 6:32 PM), http://www.mediapost.com/publications/article/214932/will-consumers-loss-against-apple-affect-other-p.html.

[185] *Id.*

[186] *Id.*

[187] *Id.*

B. Possible Reforms for Privacy Policy Laws

Accordingly, there clearly needs to be reform in the area of privacy policies, since consumer lawsuits are generally unsuccessful, and even lawsuits based on violations of privacy policies are not reliable. Consumers deserve to have a foolproof option of protecting themselves from not only floods of emails and advertisements, but from the various intrusive methods of data collection retailers employ. Another aspect that needs to be addressed is the fact that most people do not even read a website's privacy policy, and the policy is usually hard to find on the website. As an attempt to address these issues, in 2011 Senators John Kerry and John McCain initiated "The Commercial Privacy Bill of Rights Act of 2011."[188] This Bill sought to authorize the Federal Trade Commission to establish rules that require, rather than simply recommend, collectors of personally identifiable information (PII) to provide "*notice to individuals on PII collection practices and the purpose for such collection*."[189]

The Commercial Privacy Bill of Rights Act of 2011 would only apply to commercial uses of personal data, which includes data that is linkable to a specific individual.[190] This Bill establishes a set of consumer rights that "inform[s] consumers of what they should expect of companies that handle personal data."[191] However, this bill also recognizes that with an increasingly interconnected society, consumers will have to take on some responsibility to protect their own privacy.[192] Accordingly, this Bill balances these two objectives by requiring the

---

[188] Connelly, *supra* note 176.

[189] *Id.*

[190] *Consumer Data Privacy In A Networked World: A Framework For Protecting Privacy And Promoting Innovation In The Global Digital Economy*, THE WHITE HOUSE (Feb. 2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf [hereinafter *Consumer Data Privacy*].

[191] *Id.*

[192] *Id.*

content of privacy policies to include "the goals or purposes that consumers can expect to achieve by using a company's products or services, the services that the companies actually provide, the personal data exchanges that are necessary to provide these services, and whether a company's customers include children and adolescents."[193] The Bill also states that consumers have a right to individual control, transparency, respect for context, security, access and accuracy, focused collection, and accountability.[194]

With regard to individual control, this Bill would require companies to provide consumers control, upfront, over the personal data the company is able to collect from the consumer, along with the use and disclosure of that data.[195] In order to accomplish this, the Bill states that companies should provide consumers with easy and accessible mechanisms that reflect the sensitivity of the data collected.[196] In addition, the Bill claims that companies should present consumers with reasonable methods of withdrawing and limiting consent to collection of personal data.[197] This is exactly the type of regulation needed to provide consumers with the option of having their personal information collected. By requiring companies to offer this choice to consumers, litigation over privacy policies would drastically decrease.

As for transparency, this Bill states that companies should clearly assert what personal data it is collecting, the purpose for which it is collected, how the data will be used, and when it

---

[193] *Id.*

[194] *Id.*

[195] *Consumer Data Privacy*, *supra* note 190, at 11.

[196] *Id.*

[197] *Id.*

will share the data with third parties.[198] Also, regarding respect for content, this Bill maintains that companies should limit its use and disclosure of personal information to purposes consistent with the context in which the data was originally disclosed.[199] This will allow consumers to make an informed decision as to whether and what type of information to allow the company to collect, which will let consumers chose how to best protect their personal information.

Next, with regard to security, this Bill proposes that companies assess "the privacy and security risks associated with their personal data practices and maintain reasonable safeguards to control risks such as loss; unauthorized access, use, destruction, or modification; and improper disclosure."[200] This is especially important because if companies do not take safety measures with regard to privacy of consumer information, the results can be catastrophic. For example, in December 2013, hackers stole tens of millions of Target customers' credit card and personal information.[201] This resulted in millions of people having to cancel their credit cards and closely monitor their bank accounts for signs of fraud, along with a loss of faith in the Target brand.[202]

As for access and accuracy, this Bill would compel companies to use reasonable measures to ensure it maintains accurate personal data and provides consumers with access to their personal data and the opportunity to request the removal or limitation of their

[198] *Id.* at 14.

[199] *Id.* at 15.

[200] *Consumer Data Privacy*, *supra* note 190, at 19.

[201] Matthew Rocco, *Target Says Data Theft May Include 40M Cards*, FOXBUSINESS.COM (Dec. 19, 2013), http://www.foxbusiness.com/industries/2013/12/19/target-confirms-major-card-data-theft-during-thanksgiving-1487625092/.

[202] *Id.*

information.[203] This section, again, further reinforces the right of consumers to have their personal information removed from a company's database.

Concerning focused collection, this Bill would require that companies only collect the minimum amount of personal data needed to accomplish their purpose.[204] Also, once companies no longer need a consumer's personal information, the company should dispose of or de-identify it.[205] Thus, this requirement would force companies to engage in upfront decision-making about the kinds of data they need to collect to accomplish specific purposes.[206] Therefore, companies will collect no more personal data than absolutely necessary, which makes less information vulnerable to theft.

Finally, this Bill mandates the already generally accepted principle that companies should be held accountable to enforcement authorities and consumers for adhering to these principles.[207]

With regard to J.Crew's privacy policy, the company, for the most part, follows the suggestions provided in the Bill. First, as we have seen, J.Crew offers customers the option to prevent tracking and stop communications from J.Crew.[208] Also, J.Crew explicitly states the type of data it collects and why it collects such data.[209] J.Crew also states that it may share consumer information with third parties for a list of purposes.[210] As for security, J.Crew states that it takes

---

[203] *Consumer Data Privacy*, *supra* note 190, at 19.

[204] *Id.* at 21.

[205] *Id.*

[206] *Id.*

[207] *Id.*

[208] J.CREW, *supra* note 10.

[209] *Id.*

[210] *Id.*

"reasonable measures" to ensure the safety of consumer information, which is exactly what the Bill would mandate.[211] However, J.Crew does not offer any explanation for disposal or de-identification of consumer information once it is done being used by the company. Also, J.Crew's policy does not mention any accountability for adhering to the principles set forth in its privacy policy.

While this Bill was not enacted, considering the increased interest in privacy, it likely will not be long before Congress passes a similar bill, mandating accessible privacy policies, at the federal level.[212] This Bill contains provisions that are much needed to protect consumers' personal information from companies using it for inappropriate purposes or purposes for which the consumer does not intend. Going forth, the main goal of laws about privacy policies should focus on disclosure of details about the collection of consumer information, along with giving consumers the option of deciding what information the company shares and collects about them. Accordingly, in March 2012, the FTC issued a report outlining "the best practices for businesses to protect the privacy of American consumers and give them greater control over the collection and use of their personal data."[213] In addition, the FTC recommended that Congress enact "general privacy legislation, data security and breach notification legislation, and data broker legislation" in order to better protect consumer privacy.[214]

---

[211] *Id.*

[212] Commercial Privacy Bill of Rights Act of 2011, S.799, 112th Cong. (2011), *available at* https://www.govtrack.us/congress/bills/112/s799.

[213] *FTC Issues Final Comm'n Report on Protecting Consumer Privacy*, FEDERAL TRADE COMM'N (Mar. 26, 2012), http://www.ftc.gov/news-events/press-releases/2012/03/ftc-issues-final-commission-report-protecting-consumer-privacy [hereinafter *FTC*].

[214] *Id.*

C. Recommendations for Concerned Consumers

Therefore, until Congress passes a law at the federal level, requiring all companies to provide privacy policies, the following are recommendations to consumers for best protecting their privacy. First, consumers should ask a variety of questions when confronted with requests for personal information.[215] The purpose of these questions is to limit the information that companies collect.[216] Initially, consumers need to be assertive when asked for information they feel is unnecessary to complete the transaction.[217] The questions consumers should ask include: Why is this information required?; What will be done with this information?; and, What benefit do I receive for providing the company with my personal information?[218]

Furthermore, consumers should not provide non-essential personal information unless they are content with the intended use of that information.[219] Specifically, consumers should be prudent in protecting their Social Security number.[220] While some organizations have a right to demand disclosure of your Social Security number, such as federal and state revenue departments, consumers have the right to refuse to provide it to most other businesses.[221]

---

[215] *What Personal Information Should You Give to Merchants?*, PRIVACY RIGHTS CLEARINGHOUSE, https://www.privacyrights.org/what-personal-information-should-you-give-merchants (last visited Nov. 15, 2014) [hereinafter *What Personal Information*].

[216] *Id.*

[217] *Id.*

[218] *Id.*

[219] *Id.*

[220] *What Personal Information*, *supra* note 215.

[221] *Id.*

With regard to credit card security, federal law prohibits "merchants from printing more than the last five digits of an account number on a customer receipt."[222] Therefore, if a consumer discovers that a merchant is printing more data than necessary on receipts, this may be an indication that the merchant's personal information collection policies are lacking in security.[223] Another option, until a federal law concerning privacy policies is passed, is for consumers to contact their state and federal legislators and urge them to address the developing practice of merchants gathering consumer data for multiple purposes.[224]

CONCLUSION

This note has shown what the privacy policy of a mass retailer looks like and the ramifications that flow from each section. In addition, we have seen the different methods consumers can employ to enforce their privacy rights, while they might not altogether be successful. Also, we saw the results of when a company blatantly violates its own privacy policy. Furthermore, we looked at a bill that offered recommendations for best protecting consumer privacy, and while not enacted, provides the groundwork for future privacy laws. Finally, we looked at suggestions by the FTC for consumers to best protect their personal information from companies, until appropriate privacy laws are enacted. Therefore, until Congress enacts appropriate privacy laws, consumers must take it upon themselves to protect their personal information from unacceptable use by retailers and companies seeking to make money.

[222] *Id.*

[223] *Id.*

[224] *Id.*

SYRACUSE JOURNAL OF SCIENCE & TECHNOLOGY LAW

VOLUME 31 2014-2015 ARTICLE 2, PAGE 39

TRAGEDY OF THE COMMONS: SNOWDEN'S REFORMATION AND THE BALKANIZATION OF THE INTERNET

MATTHEW FUNK

"Thou hast loosed an Act upon the world, and as a stone thrown into a pool so spread the consequences thou canst not tell how far." –Rudyard Kipling[1]

INTRODUCTION

In 1517, Martin Luther put into motion events that would uproot the hegemony of the Catholic Church in Western religion.[2] His *Ninety-Five Theses* would be the basis for an enormous upheaval of the sacred status quo, and challenge centuries of religious ordering. His "protest" of the practices of the Catholic Church would be disseminated with the power of the printing press, the pinnacle of information technology at the time, and lead to a great fork in the history of Christianity. Protestantism, with unique movements springing up throughout Europe, would ultimately separate from the oversight of the Catholic Church and create a new religious paradigm.

No different in principle, but perhaps in scale, has been the upheaval caused by the confessions of former National Security Agency contractor Edward Snowden. His "leak of [National Security] [A]gency documents has set off a . . . debate over the proper limits of

[1] RUDYARD KIPLING, KIM: AUTHORITATIVE TEXT, BACKGROUNDS, CRITICISM 176 (Zohreh T. Sullivan ed., 2002).

[2] *See generally*, Geoffrey Parker, *Success and Failure during the First Century of the Reformation*, 136 PAST & PRESENT 43, 82 (1992), *available at http*://past.oxfordjournals.org/content/136/1/43.full.pdf+html (describing the early developments of the Protestant Reformation).

government surveillance."[3] These leaks have "opened an unprecedented window on the details of surveillance by the NSA, including its compilation of logs of virtually all telephone companies in the United States and its collection of e-mails of foreigners from the major American Internet companies."[4] This, in turn, has rippled into raucous calls for a new Reformation—one of Internet, not religious, sovereignty and sensibilities. Such calls implicate the principles undergirding the purposes, governance, and even geography of the Internet. And while the calls may not lead to a catastrophic schism on the scale of Christianity's division in the 16th century, they are certainly loud enough not only to question policy choices regarding the defining information technology of the new millennium thus far, but also to challenge the traditional dynamics of sovereignty-retention in the face of a global online commons.

States, and their behavior in the modern world, are geopolitically defined in territorial terms. This territorial approach was "accepted as the primary political strategy after the anarchic implications of a negative-sum game . . . became widely appreciated."[5] At the state level, "the content of a territory can be manipulated and its character designed," and this territory can be used "as the instrument for securing a particular outcome."[6] The modern territorial state, forged by trial-and-error over the past two centuries, seeks to maximize if not monopolize control and power over achieving these particular outcomes. It has thus emerged as a "power container," predicated on the "domination of political practice in the world by territoriality" as a

---

[3] Scott Shane, *Ex-Contractor Is Charged in Leaks on N.S.A. Surveillance*, N. Y. TIMES (June 21, 2013), http://www.nytimes.com/2013/06/22/us/snowden-espionage-act.html?adxnnl=1&adxnnlx= 1385312525-3kfeFqdcTH4zPWJ2P5KjTg.

[4] *Id.*

[5] Peter Taylor, *The state as container: territoriality in the modern world-system*, 18 PROGRESS IN HUMAN GEOGRAPHY, 151, 161 (1994), *available at* http://phg.sagepub.com/content/18/2/151.full.pdf+html.

[6] *Id.* at 151.

"consequence of [the] territorial link between sovereign territory and national homeland."[7] States as power containers can be "filled" or "leak," by the successes or failures, respectively, of their four basic tasks: waging war, managing the economy, giving national identity, and providing social services.[8] These successes or failures amount to state "containment of power, wealth, culture, and society"[9] respectively.

The modern state's relationship with the Internet fits neatly within territoriality theory. Despite its origins in the security apparatus of the United States, and its initial purpose as a tool for war-making power accumulation, the Internet has come to represent, in some respects, a leak in the power container of the modern state. This is, for the most part, due to its nature as a globally accessible information technology and its continued development away from traditional norms of territoriality and the physical geopolitical borders observed by states. For many states and individuals alike, this globalization pushes away from the constructed and imagined communities that exist at the state level.[10]

The Internet will continue, consequently, to poke holes in the modern state as a power container unless respective sovereign authorities are able to plug them and recapture the true filling potential of the Internet by maximizing their own control locally while minimizing influence from beyond their borders. The Internet today has no fewer than 2.4 billion users (roughly 34% of the world's population),[11] and is a tool that has truly interpenetrated the border

---

[7] *Id.*

[8] *See id.* at 152 (citing the four basic tasks of the modern nation-state).

[9] *Id.*

[10] *See* Taylor, *supra* note 5, at 155 (discussing nations, in Benedict Anderson's famous phrase, as "imagined communities").

[11] *See Internet Usage Statistics*, INTERNET WORLD STATS, http://internetworldstats.com/stats.htm (last updated Dec. 31, 2013) (providing global Internet usage statistics).

between the real and the virtual."[12] For some, this "conflict between states as containers and the global ecosystem is interpreted as leading to a future end of the state," while for others, "territoriality is too good a strategy to dispatch to history."[13]

The viability of either theory and either outcome is not yet clear, but the importance of state responses to the Snowden leaks certainly is. States are realizing diminished levels of sovereignty and control over domestic online activity via third-party surveillance actors – holes in their power containers. In addition to the traditional practice of censorship, there is now another half of the equation when it comes to maintaining territoriality online: containment of local resources and data to the preclusion of prying eyes. Whether an ultimate balkanization of online interests is to befall the Internet as a result of these containment efforts will be determined by the subsequent choices states have, and will continue to make in response to such realizations of susceptibility.

I. HISTORICAL DEVELOPMENT OF THE INTERNET

Before the implications of the Snowden leaks can be assessed, the guiding principles adopted and policy choices made by the U.S. Department of Defense in the early development of the Internet must be understood. At the most basic level, the Internet is a "packet switched communications facility in which a number of distinguishable networks are connected together using packet communications processors called gateways which implement a store and forward packet forwarding algorithm."[14] ARPANET, the first iteration of today's Internet, was designed

---

[12] Barney Warf, *Geographies of Global Internet Censorship*, 76 GEOJOURNAL, 1, 1 (2011) *available at* http://link.springer.com/article/10.1007%2Fs10708-010-9393-3#page-1.

[13] Taylor, *supra* note 5, at 152.

[14] David Clark, *The Design Philosophy of the DARPA Internet Protocols*, ACM SIGCOMM, 2 (1988), http://ccr.sigcomm.org/archive/1995/jan95/ccr-9501-clark.pdf.

"to come to grips with the problem of integrating a number of separately administered entities into a common utility"[15] and develop "an effective technique for multiplexed utilization of existing interconnected networks."[16]

Notwithstanding the fundamental goal of connecting preexisting networks, early policy decisions within the Department of Defense prioritized some features over others.[17] In order of importance:

> 1. Internet communications must continue despite loss of networks or gateways; 2. The Internet must support multiple types of communications service; 3. The Internet architecture must accommodate a variety of networks; 4. The Internet architecture must permit distributed management of its resources; 5. The Internet architecture must be cost effective; 6. The Internet architecture must permit host attachment with a low level of effort; 7. The resources used in the Internet architecture must be accountable.[18]

A commercial network would certainly reorder such goals, but it is always worth remembering ARPANET "was designed to operate in a military context."[19]

In terms of the Internet developing as a commons that was to depart from traditional notions of territoriality, goals two, three, four, and five are the most pertinent. These represent the accommodation of a variety of communications services and networks, distribution of resource management, and cost-effectiveness. Such features, though originally military-minded priorities, created the basis for a thriving, global Internet in a setting where approaches, standards, and allocable resources would come to vary widely.

---

[15] *Id.*

[16] *Id.* at 1.

[17] *Id.* at 2.

[18] *Id.*

[19] Clark, *supra* note 13, at 2

Because ARPANET was developed along guiding principles that fostered a global-commons model, state power containers leaked politically, economically, and socially as adoption of the Internet progressed. Politically, the Internet "necessarily and inevitably promotes democracy by giving voice to those who lack political power."[20] Economically, commercial actors around the world embraced "convenient access to worldwide information," the possibility of "establishing a global presence," and "extending world market reach,"[21] resulting in "rapid globalization of economic activities that has made territorial economic containment"[22] increasingly difficult. Socially, global adoption has led to rampant cultural diffusion, cutting severely against the idea of roughly two hundred distinct cultural containers, "within which national ideals are being reproduced in schooling, the mass media and all manner of other social institutions."[23] The Internet, from the start, has come to represent a leaky reality for the modern power container.

Despite these realities, the Internet was and is celebrated at for its decentralized, multi-stakeholder model, named so because "businesses, organizations, governments, and users all play their part"[24] in Internet governance. For about ten years, the Internet "completely overcame the telecommunications system of national boundaries . . . a virtual space that was completely interconnected and globalized, and governments had to react to that after the fact."[25] With only

[20] Warf, *supra* note 12, at 2.

[21] Margaret Tan and Thompson S.H. Teo, *Factors Influencing the Adoption of the Internet*, INT'L J. OF ELECTRONIC COM. 5, 10 (Spring 1998), *available at* http://www.jstor.org/stable/pdfplus/27750854.pdf?acceptTC=true&acceptTC=true&jpdConfirm=true.

[22] Taylor, *supra* note 5, at 158.

[23] *Id.* at 156.

[24] Marietje Schaake, *Stop Balkanizing the Internet*, HUFFINGTON POST (July 17, 2012, 10:59 AM), http://www.huffingtonpost.com/marietje-schaake/stop-balkanizing-the-internet_b_1661164.html.

one organization, ICANN, in a significant position of governance, the multi-stakeholder model "defies top-down control"[26] and "simply does not care about traditional borders."[27] This has been the status quo since the mass adoption of the Internet as an information technology, and is not to say that states have not attempted, vehemently even, to territorialize online spaces and stop the leaking.

II. STATE ASSERTIONS OF SOVEREIGNTY OVER DIGITAL TERRITORY

Given the leaky potential of the Internet as an information technology, it is no surprise that state sovereign authorities have attempted to use it instead to fill their containers. Traditionally, this has been in the form of state governments restricting what *outside* information users *inside* their territory have access to (i.e. censorship), to better control what information can be disseminated to and among their citizens. However, after watershed revelations regarding NSA practices, states are now looking to restrict what *inside* information users *outside* their territory have access to (i.e. containment), an attempt to reestablish sovereignty over content produced within their borders by citizens susceptible to surveillance by third parties. While not necessarily employed by all states, both mechanisms, censorship and containment, are two sides

[25] Tom Gjelten, *Are We Moving To A World With More Online Surveillance?*, NPR (Oct. 16, 2013, 2:56 AM), http://www.npr.org/blogs/parallels/2013/10/16/232181204/are-we-moving-to-a-world-with-more-online-surveillance?sc=17&f=1001.

[26] Steven Titch, *We Must Take UN's Internet Grab Seriously*, REASON FOUNDATION (June 21, 2012, 5:06 PM), http://reason.org/blog/show/1012962.html. That is not to discount the importance of regulation at some level. *See* Zoë Baird, *Governing the Internet- Engaging Government, Business, and Nonprofits*, FOREIGN AFFAIRS, 18 (Dec. 2002), *available at* http://www.jstor.org/stable/pdfplus/20033341.pdf?acceptTC=true&acceptTC=true&jpdConfirm=true (noting the importance of bureaucratic administration on the part of ICANN).

[27] Schaake, *supra* note 24.

of the same coin and together represent the complete picture of territorial practices in digital spaces.[28]

A. The Era of Censorship: Territoriality Before Snowden

Traditional manifestations of online territorial behavior by states are most often reflected in attempts by governments to control virtual behavior within their borders, just as they might attempt to control physical behavior. Authoritarian and politically repressive governments most "often fear the emancipatory potential of the Internet, which allows individuals," to some extent, "to circumvent tightly controlled media."[29] In this sense, the "world's authoritarians have shown just as much aptitude for technology as their discontented citizens"[30] as they move to centralize power online for political, religious, economic, and moral reasons. However restrictive censorship policies may be, whether they are more like Denmark's with a completely unrestricted Internet or North Korea's with no access whatsoever,[31] it remains true that "only 13% of the world's people . . . live in countries with minimal censorship," while "one quarter of the world's people and Internet users live under governments that engage in very heavy censorship."[32]

At the most basic level, censorship entails control over Internet "access, functionality, and contents."[33] Because precise filtering is relatively difficult, censorship tends to take on many

[28] States, of course, make value judgments in theory about what type of regime they wish to employ in practice, so levels of censorship and containment operate on a sliding scale depending on levels of desired involvement, protectionism, or involvement.

[29] Warf, *supra* note 12, at 3.

[30] *Id.*

[31] *Id.* at 4.

[32] *Id.* at 5.

forms, including content filtering based on keywords, redirection, website blocking, discriminatory pricing, hardware and software manipulation, spreading viruses, denial-of-service attacks, and even just-in-time blocking at moments when political information is critical.[34] Almost ubiquitous, however, is "self-censorship," where users police their own behavior out of fear of repercussions, or even out of habit.[35] Censorship could also conceivably be used as a means of containment, where access to services known to be bugged could be blocked. No matter the form it takes, however, censorship is and always will be susceptible to mission creep; "[o]nce formal censorship is initiated, no matter how benign or transparent, the temptation to enlarge its scope . . . is always there."[36]

The same various methods of censorship may be employed across countries, but states each take their own unique approach to the traditional, censorship-based attempts at territoriality online. To use the United States as an example, sanctioned censorship efforts in the U.S. largely revolve around controlling negative externalities "such as Internet crime and pornography that the market, left to its own devices, would fail to control."[37] Additionally, the FBI "encourages ISP's to censor websites that are not consonant with the public interest and to turn over information about users whose email reveals suspicious intent."[38]

China, on the other hand, with more than 420 million Internet users arguably has the world's most severe Internet censorship.[39] Since 2006, China's "Great Firewall" has been the

---

[33] *Id.* at 4.

[34] *See* Warf, *supra* note 12, at 4 (explaining the various methods of Internet censorship).

[35] *Id.*

[36] *Id.*

[37] *Id.* at 8.

[38] *Id.*

"most extensive, technologically sophisticated, and broad-reaching system of Internet filtering in the world."[40] State controlled backbone networks control all international Internet connections, while monitors and citizen volunteers (Beijing alone has 10,000) screen "blogs and email messages for potential threats to the established political order," and access to popular services like Yahoo! and Google is heavily restricted.[41]

Russia, too, was "never all that supportive of Internet freedom."[42] While it certainly lacks the extensive infrastructure that Chinese censorship programs employ, the Russian system relies heavily, as many censorship regimes do, on self-censorship. "Russia's Internet surveillance law . . . allows state security services unfettered physical access to ISPs and requires them to report statistics about users."[43] This is all supposedly in the name of "fighting corruption."[44] Reported statistics create self-policing behavior on the part of users who fear that their activities online have the potential of becoming known to government authorities.

While China relies heavily on infrastructure at the state level and Russia relies on self-censorship at the individual level, Iran "manages its censorship at the level of the ISP."[45] Not only has the government "assumed control over all international traffic entering or leaving the country," but ISP's must also prohibit access to all "non-Islamic" websites. Together, these three regimes represent the various levels at which online censorship can be executed: state, individual,

[39] Warf, *supra* note 12, at 8.

[40] *Id.*

[41] *Id.*

[42] Gjelten, *supra* note 25.

[43] Warf, *supra* note 12, at 11.

[44] *Id.*

[45] *Id.* at 10.

and ISP. This was the traditional approach to territoriality and power container theory online, but after Snowden, another side of the coin was revealed.

B. Watershed: What the NSA Did and Why It Matters

The documents leaked by Edward Snowden in the summer of 2013 set off a chain of events that would lead to a dramatic change in the way both individuals and states look at the Internet. This involved the exposure of "hundreds of classified documents" pointing to what Snowden believed to be a shocking "invasion of Americans' and foreigners' privacy."[46] Snowden has since sought asylum abroad, but the effects of his disclosures remain.

Documents he provided reveal that the NSA employed an elaborate surveillance network that "cracked much of the online encryption relied upon by hundreds of millions of people to protect the privacy of their personal data, online transactions and emails."[47] To achieve this, the NSA uses Computer Network Exploitation (CNE), the "secret infiltration of computer systems achieved by installing malware."[48] CNE was used on "more than 50,000 computer networks worldwide," specifically "designed to steal sensitive information."[49] Thousands of officers, housed within the NSA's TAO (Tailored Access Operations) division execute the agency's CNE surveillance, some of which has been ongoing since as early as 1998 and reached users as far away as Brazil and Venezuela.[50] The documents also implicate the NSA's use of

---

[46] Shane*, supra* note 3.

[47] James Ball, Julian Borger & Glenn Greenwald, *Revealed: how US and UK spy agencies defeat internet privacy and security*, THE GUARDIAN (Sept. 5, 2013), http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security (noting the NSA's high cyber-surveillance budget).

[48] Floor Boon, Steven Derix & Huib Modderkolk, *NSA infected 50,000 computer networks with malicious software*, NRC (Nov. 23, 2013, 2:40 AM), http://www.nrc.nl/nieuws/2013/11/23/nsa-infected-50000-computer-networks-with-malicious-software/.

[49] *Id.*

[50] *See id.* (noting the long history of the NSA's surveillance program).

"supercomputers to break encryption with 'brute force'" and NSA collaboration with technology companies and service providers" to insert exploitable vulnerabilities.[51] Aside from the undoubtedly large personnel costs, such methods of surveillance are "relatively inexpensive" yet "provide the NSA with opportunities to obtain information that they otherwise would not have access to."[52]

Smartphones, however, are the NSA's goldmine. Notwithstanding the fact that half of American, half of German, and two-thirds of British citizens have one, smartphones combine "in a single device almost all the information that would interest an intelligence agency: social contacts, details about the user's behavior and location, interests (through search terms, for example), photos and sometimes credit card numbers and passwords."[53] Realizing the surveillance potential of the smartphone's meteoric rise in popularity, the NSA set up task forces for tapping "leading smartphone manufacturers and operating systems," like Blackberry, Apple's iOS, and Google's Android.[54] Such surveillance programs are also not solely limited to United States government agencies—they have also been revealed, for example, in Great Britain, Sweden, and the Netherlands.[55]

---

[51] *See* Ball, *supra* note 47 (explaining the various NSA surveillance techniques).
[52] *Id.*

[53] Marcel Rosenbach, *How the NSA Accesses Smartphone Data*, SPIEGEL ONLINE (Sept. 9. 2013, 12:25 PM), http://www.spiegel.de/international/world/how-the-nsa-spies-on-smartphones-including-the-blackberry-a-921161.html.

[54] *Id.*

[55] *See* Ball, *supra* note 47 (noting the existence of the British surveillance program); Gunnar Rensfeldt, *FRA has access to controversial surveillance system*, SVT (Dec. 11, 2013, 2:39 PM), http://www.svt.se/ug/fra-has-access-to-controversial-surveillance-system (Swedish program); Steven Derix, Glenn Greenwald & Huib Modderkolk, *Dutch intelligence agency AIVD hacks internet forums*, NRC (Nov. 30, 2013, 3:00 AM), http://www.nrc.nl/nieuws/2013/11/30/dutch-intelligence-agency-aivd-hacks-internet-fora/?ref=twt2 (Dutch program).

The fruits of these labors are quite intrusive—"an image of a former defense secretary with his arm around a young woman;" images depicting "young men and women in crisis zones, including an armed man in the mountains of Afghanistan;" and "an Afghan with friends and a suspect in Thailand."[56] These cited examples all implicate private individuals, but it seems officials of foreign governments have been targeted as well. The German government recently "awarded a major contract for secure mobile communications within federal agencies" to Blackberry, one of the operating systems cracked by NSA task forces. Whether created by individuals in a private or public capacity, smartphone data can be tapped either from the phone itself, or from backup files created by users on their computer.[57] The documents leaked by Snowden certainly paint a startling picture of what modern surveillance techniques can accomplish when agencies are given access to copious resources.[58]

Symbolically, however, the unveiling of extensive government surveillance programs has and will continue to have far-reaching implications. The NSA and similar programs have subverted "the internet and turn[ed] it into a massive surveillance tool." This has both challenged previous beliefs that cryptography could be used to create a "basis for trust online," and undermined "the very fabric of the internet."[59] This lack of trust will, in turn, drive countries towards domestic technology companies that "require citizen data to stay within their borders."[60] Not to mention the fact that all users, and no longer just those in known surveillance states, will

---

[56] Rosenbach, *supra* note 53.
[57] See *id.* (explaining how such tactics are employed).

[58] *See* Ball, *supra* note 47 (citing the $250 million dollar annual budget of a single NSA program).

[59] *Id.*

[60] Grant Gross, *US faces major Internet image problem, former gov't official says*, COMPUTERWORLD (Dec. 5, 2013, 4:48 PM), http://www.computerworld.com.au/article/533605/us_faces_major_internet_image_problem_former_gov_t_official_says/.

"think twice about what opinions to express" online.[61] While the constitutionality of the NSA programs is still unclear,[62] the existence of palpable effects on user behavior in digital spaces is undoubted. Internet users in all corners of the globe are potentially vulnerable to surveillance as long as NSA and similar government programs remain in effect.

C. A New Era: Territoriality Online After Snowden

These leaky vulnerabilities have inspired responses from private and public actors alike, new approaches to protecting the integrity of the territorial state as power container in the digital age. Such realizations of vulnerability, though, have prompted territorial behavior most visibly in liberal governments and only residually in more repressive states.[63] This type of behavior was traditionally reserved for authoritarian regimes engaging in censorship. Regardless of practitioner, though, the NSA-effected containment efforts have brought into existence a new manifestation of territorialism online. Snowden's confession turned over the coin of digital territoriality from censorship to containment.

Since Snowden's disclosures, Brazil has been out in front of online containment efforts. The Brazilian government learned that the NSA has led extensive surveillance efforts there,[64] going so far as to target private emails and calls,[65] the Brazilian president, Dilma Rousseff,[66] and

---

[61] *Id.*

[62] *See* Josh Gerstin, *Judge: NSA phone program likely unconstitutional*, POLITICO (Dec. 16, 2013, 1:36 PM), http://www.politico.com/story/2013/12/national-security-agency-phones-judge-101203.html (predicting that U.S. constitutional issues will go unresolved until a case on point goes before the Supreme Court).

[63] *See* Scott J. Shackelford, *The Coming Age of Internet Sovereignty?*, HUFFINGTON POST (Jan. 10, 2013 6:59 PM), http://www.huffingtonpost.com/scott-j-shackelford/internet-sovereignty_b_2420719.html (discussing Iran's recent containment policies); Gjelten, *supra* note 25 (discussing Russia and China's recent containment policies).

[64] *See* Boon, *supra* note 48 (citing an NSA presentation that revealed CNE surveillance targets).

[65] *See* Leo Kelion, *Brazil plans secure email service to thwart cyber-spies*, BBC NEWS (Oct. 14, 2013), http://www.bbc.co.uk/news/technology-24519969 (explaining the NSA's targeting of private Brazilian communications).

domestic oil giant Petrobas.[67] President Rousseff herself has led the charge, "fast-tracking a vote on a once-dormant bill that could require that data about Brazilians be stored on servers in the country."[68] This would involve the Brazilian government requiring service providers to "keep the servers in Brazil, encrypt all the traffic inside or outside the country, and only give access to Brazilian police and intelligence services."[69] While it is clear that many state actors find NSA practices unpalatable, it "has touched a real nerve in Brazil, a country that prizes its sovereignty and is understandably sensitive about such abuses."[70] In Rousseff's own words, "the relationship [Brazil has with the U.S.], based on the fact that [they] are big democracies in this part of the world, is incompatible with the act of spying."[71] Brazil has consequently sought to reestablish territoriality over its digital spaces, not with censorship, but with containment.

While Brazil has been weighing its options south of the equator, Europeans in the northern hemisphere are making similar containment-oriented decisions. Like in Brazil, the Finnish public sector has stepped in to mollify concerns of foreign data surveillance. The Finnish government has announced plans to "build a fast, high-quality and cyber-secure connection to European and global networks from Finland to Germany via an underwater fibre optic cable."[72]

---

[66] *See* Gjelten, *supra* note 25 (discussing the reactions of various states and leaders to the extent of NSA programs).

[67] Juan Forero, *Brazilian TV show says U.S. spied on state-run Petrobras oil firm, cites NSA*, WASH. POST (Sept. 8, 2013), *available at* http://articles.washingtonpost.com/2013-09-08/world/41880912_1_petrobras-obama-administration-president-obama.

[68] Elizabeth Dwoskin & Frances Robinson, *NSA Internet Spying Sparks Race to Create Offshore Havens for Data Privacy*, WALL ST. J. (Sept. 27, 2013, 12:15 PM), http://online.wsj.com/news/articles/SB10001424052702303983904579096082938662594.

[69] Kelion, *supra* note 65.

[70] Dwoskin, *supra* note 68.

[71] *Id.*

[72] *New data cable to make Finland's one of the world's most attractive ICT regions*, FINNISH GOV'T. (Nov. 12, 2013, 2:30 PM), http://government.fi/ajankohtaista/tiedotteet/tiedote/en.jsp?oid=402176.

Such a cable would "raise the protection of Finland's international connections and data security to a new level"[73] through preclusive containment measures.

In Germany, it has been the private, not public sector that has responded to security concerns after the surveillance susceptibilities of citizens' user data became known.[74] Three of the largest email providers in Germany, recognizing the potential market for such a service, jointly developed "Email Made in Germany. The companies promise that by encrypting email through German servers and hewing to the country's strict privacy laws, U.S. authorities won't easily be able to pry inside."[75] Within two months of Email Made in Germany's release, more "than a hundred thousand Germans [had] flocked to the service."[76]

In addition to the liberal-state public and private sectors, there is also a third flavor of containment advocate: bandwagon authoritarian states trying to capitalize on the growing balkanization movement. Known traditionally for their censorship practices, these states would benefit from containment in that with greater balkanization and a rise in the popularity of territorial containment practices online there would be less transparency from the outside looking in on their regulation of digital spaces should they also choose to adopt such policies. Iran, considering perhaps the most extreme approach, is reportedly "building a national network detached from the global Internet to enhance government control of information and potentially better guard against cyber attacks."[77] Russia and China are also pushing to "centralize their

---

[73] *Id.*

[74] *See* Rosenbach, *supra* note 53 (noting the vulnerabilities of German public officials, who use NSA-cracked Blackberry devices and software)

[75] Dwoskin, *supra* note 68. *See also Verschlüsselung*, EMAIL MADE IN GER., http://www.e-mail-made-in-germany.de/ (last visited Mar. 9, 2015) (describing the service's encoding mechanism).

[76] Dwoskin, *supra* note 68.

[77] Shackelford, *supra* note 63.

[Internet] infrastructures and get the U.S. out of the picture."[78] With increased balkanization among capitalizing repressive states, such practices could "have negative consequences for free speech as well as for protection of privacy."[79] The Internet would move away from the auspices of the vulnerable, yet free-speech driven, U.S. dominated model and towards individualized centralization under authoritarian regimes like those of Iran, Russia, and China already employing and benefiting from digitally restrictive policies.

Regardless of actor, regime, or motivation, reactionary containment efforts have already catalyzed the potential balkanization of online resources. This represents a straying from the idea of a global commons that has flourished since the early days of the Internet and towards the colonization and retainment of digital spaces spaces under individualized regimes. As states move to stake their claim in the digital commons, asserting territoriality in twenty-first century fashion, it remains to be seen how far states will go to protect the integrity of their power containers against the draining practices used by those beyond.

III. FUTURE DEVELOPMENTS

Balkanization efforts by states seeking to contain proprietary digital resources put the traditional, multi-stakeholder model of the Internet at risk. Many states, like Brazil, Finland, and Germany, would like to see an expansion of the twentieth-century power container to include a more rigorous exaction of control over twenty-first century digital resources. For these states, policy choices have laid the groundwork for a more state-centric approach to the geography of online spaces, data, and politics, leading to a dramatic evaluation of the state of the Internet today. States have called into question that ordering of priorities affected by the Department of

[78] Gjelten, *supra* note 25.
[79] *Id.*

Defense in the creation of ARPANET, and the subsequent development of a decentralized, colonized global commons. Whether the state-centric model succeeds in its usurpation or the multi-stakeholder model manages to retain its preeminence will be determined ultimately by evaluations of the two approaches.

At its heart, the state-centric model aims to apply power container and territoriality theory to achieve the centralization of Internet resources under a particular regime. This would result in an increased balkanization of digital spaces among individual sovereigns. The states employing reactionary measures do so in the belief that "everyone's data and privacy are more vulnerable to hackers, governments, terrorists, and criminals of all kinds" due to NSA installation of not only secret back doors in online services, but also manufactured weaknesses in global encryption standards.[80] Responses like those of the Brazilian and Finnish governments are "touted as a way to protect . . . citizens . . . and sovereignty"[81] by limiting the power and influence of outside actors through networked insulation. The state-centric model would trade off perceived efficiencies created by a freely discursive global marketplace for protection of domestic digital, proprietary resources that have been increasingly threatened since the advent of the Internet.

The state-centric model, though, leaves some questions unanswered. For example, "what costs will this impose in terms of innovation an interconnectedness, and how can we manage the growing reach of the leviathan to minimize distortions and protect civil liberties?"[82] Containment policies could "raise the cost of computing"[83] by establishing a system similar to "the European train system, where varying voltage and 20 different types of signaling technologies force

[80] T.A. Ridout, *Marco Civil: Brazil's Push to Govern the Internet*, HUFFINGTON POST (Oct. 22, 2013, 1:47 PM), http://www.huffingtonpost.com/t-a-ridout/brazils-push-to-govern-the-internet_b_4133811.html.

[81] *Id.*

[82] Shackelford, *supra* note 63.

[83] Dwoskin, *supra* note 68.

operators to stop and switch systems or even to another locomotive, resulting in delays, inefficiencies, and higher costs."[84] A system of countries advocating for domestic hosting like Brazil "could have trouble competing with the economies of scale enjoyed by big U.S. companies."[85]

In addition to raising costs, the varying jurisdictions of a balkanized Internet would create a new set of privacy concerns and potential rights abuses.[86] In the countries that "don't protect the privacy of citizens' Internet data" to begin with, Internet users could be safer from the eyes of outsiders, but they "wouldn't be safe from their own governments' eyes."[87] In states like Iran, Russia, and China where censorship-based territorial policies are already in effect, there could be "even less access to basic communications, hampering the ability to interact online outside of [a] regime's control and censorship"[88] with the addition of containment policies. Even Brazil, ironically enough, makes hundreds of requests for Facebook user data each year, and it would be the Brazilian government in charge of the domestic data servers. [89]

For many, though, the answer is simply to curb the use of unlawful outside surveillance. As a solution, it would theoretically maintain the integrity of states' sovereignty and reduce threats to digital power containment within a given territory. The UN, for example, recently created a right to privacy, establishing "that human rights should prevail irrespective of the

---

[84] Sascha Meinrath, *The Balkanized Internet and the Vitamin C Cartel*, THE WEEKLY WONK (Oct. 10, 2013), http://weeklywonk.newamerica.net/editions/the-balkanized-internet-the-vitamin-c-cartel/.

[85] Dwoskin, *supra* note 68.

[86] *See* Meinrath, *supra* note 84 (discussing the rights-based costs of Internet balkanization); Dwoskin, *supra* note 68 (commenting on privacy risks).

[87] Dwoskin, *supra* note 68.

[88] Meinrath, *supra* note 84.

[89] *See* Dwoskin, *supra* note 68 (discussing the Brazilian government's current data surveillance practices and proposed containment policies).

medium and therefore need to be protected both offline and online."[90] A "restoration of balance that prioritizes civil rights, not surveillance, as vital to (inter)national security"[91] could mollify the concerns of those states pushing for greater balkanization and prevent the degradation of those benefits the Internet confers as a common space under the multi-stakeholder model. At least in the case of the United States, policy-makers should ask themselves whether "the benefit of spying on Brazil's oil company [is] worth the cost of antagonizing the people of [the Western] hemisphere's second-largest democracy and giving China and Russia the moral high ground in debates over how people around the world should access information."[92] Like nuclear non-proliferation, transparently coordinating a reduction of international surveillance practices could remove the perverse incentives to balkanize and preserve the integrity of shared digital resources against containment.

CONCLUSION

The territorial approach to modern statehood was developed, as described above, in response to a "negative-sum game."[93] That negative-sum game was the Thirty-Years War that ravaged Europe, in the name of religion, a hundred years after Martin Luther catalyzed the Protestant Reformation. It was only in 1648 at the Treaty of Westphalia that the war came to an end, and where "state centralization was accepted through the principal of noninterference in each other's internal affairs, thus formally eliminating all rival power centres in [state]

---

[90] United Nations, *Third Committee Approves Text Titled 'Right to Privacy in the Digital Age', As it Takes Action on 18 Draft Resolutions*, UNITED NATIONS MEETINGS COVERAGE AND PRESS RELEASES (Nov. 26, 2013), http://www.un.org/press/en/2013/gashc4094.doc.htm.

[91] Meinrath, *supra* note 84.

[92] *Id.*

[93] Taylor, *supra* note 5, at 161.

territories."[94] With these formal recognitions, the modern sovereign state as power container could come into fruition and freely govern those territories within its borders.

Not only has the second decade of the twenty-first century seen the advent of a crystallizing digital reformation, but also the same competitively disrespectful and meddlesome state of affairs that instigates bloody, rivalrous conflicts. In order to preserve the wondrously successful sprawling commons model of the Internet, the necessity for a new Treaty of Westphalia is painfully clear. Without the same principles of restraint and noninterference governing surveillance temptations, states will have no option but to push away from each other, colonizing and centralizing digital spaces under their own regimes. It is not just the modern power container that is leaking—the limitless potential of perhaps the greatest technology the world has ever seen leaks too. To stop the leaking we must look into our past, and thus preserve our future.

[94] *Id.*

SYRACUSE JOURNAL OF SCIENCE & TECHNOLOGY LAW

VOLUME 31 2014-2015 ARTICLE 3, PAGE 60

THE SECOND AMENDMENT IMPLICATIONS OF REGULATING 3D PRINTED FIREARMS

Michael L. Smith

ABSTRACT

3D printed firearms have arrived, and commentators are beginning to ask whether and how this new technology can be regulated. An inevitable question that governments and courts will need to confront when considering restrictions on 3D printed firearms is whether these restrictions violate the Second Amendment. In this paper, I argue that most restrictions on 3D printed firearms would survive Second Amendment challenges. In carrying out this argument, I consider a complete ban on the manufacturing and possession of 3D printed firearms, and conclude that even this complete ban would be likely to survive Second Amendment challenges. Because these particularly restrictive bans are likely to survive, I conclude that most restrictions on 3D printed firearms will survive similar challenges. The main obstacle for governments will not be overcoming Second Amendment arguments against restrictions on 3D printed firearms, but ensuring that these restrictions are effective.

INTRODUCTION

On May 1, 2013, the first firearm that had ever been produced with a 3D printer was successfully fired.[1] Several weeks later, an engineer in Wisconsin used his own (relatively) cheap personal 3D printer to make a firearm that successfully fired nine shots.[2] These two developments generated national media attention and prompted calls for restrictions on 3D printed firearms. But critics responded by arguing that restricting 3D printed firearms would violate the Second Amendment right to keep and bear arms.[3]

The issue of the Second Amendment implications of 3D printed firearms combines an emerging and evolving area of the law with an even more cutting-edge area of technology. The Second Amendment as an individual right is a recent development: before the Supreme Court's 2008 decision, *District of Columbia v. Heller*,[4] it was far from clear whether the Second Amendment protected an individual right.[5] In the wake of the Court's decision in *Heller*, and its

---

[1] Andy Greenberg, *Meet the "Liberator": Test-Firing the World's First Fully 3D-Printed Gun*, FORBES (May 5, 2013, 5:30 PM) http://www.forbes.com/sites/andygreenberg/2013/05/05/meet-the-liberator-test-firing-the-worlds-first-fully-3d-printed-gun/.

[2] Andy Greenberg, *$25 Gun Created With Cheap 3D Printer Fires Nine Shots (Video)*, FORBES, (May 20, 2013, 11:51 AM), http://www.forbes.com/sites/andygreenberg/2013/05/20/25-gun-created-with-cheap-3d-printer-fires-nine-shots-video/. The printer this engineer used was a $1,725.00 "Lulzbot" printer, which was far cheaper than the $8,000.00 printer that had been used to produce the first working 3D printed firearm. *Id.*

[3] *See NRA Statement on the Reauthorization of the "Undetectable Firearms Act", HR 3626*, NRA-ILA INSTITUTE FOR LEGISLATIVE ACTION (Dec. 3, 2013), http://www.nraila.org/news-issues/news-from-nra-ila/2013/12/nra-statement-on-the-reauthorization-of-the-undetectable-firearms-act-hr-3626.aspx.

[4] 554 U.S. 570 (2008).

[5] For an outline of the debate between the individual right theorists and the group right theorists, *see* ADAM WINKLER, GUNFIGHT: THE BATTLE OVER THE RIGHT TO BEAR ARMS IN AMERICA 106-13 (W.W. Norton & Co. eds., 1st ed. 2011). For an example of scholarship from the time that took the individual right position, *see, e.g.*, Robert E. Shalhope, *The Armed Citizen in the Early Republic*, 49 L. & CONTEMP. PROB., no. 1 (1986) 138-39 (exploring whether the Second Amendment protected a militia's right to bear arms or an individual right and concluding that both rights are protected).

incorporation of Second Amendment rights to the states in *McDonald v. City of Chicago*,[6] there has been an explosion in scholarly coverage of the Second Amendment as commentators attempt to draw out the implications and limits of the individual right to bear arms. 3D printing is an even more recent development – and courts and commentators are just beginning to address issues that this technology will raise.

In this article, I will explore the Second Amendment implications of regulating 3D printed firearms. Despite the rapidly developing state of Second Amendment law and 3D printing technology, it is possible to apply trends in existing Second Amendment case law to the current and future development of 3D printed firearms. In particular, I will explore the Second Amendment implications of a complete ban on 3D printed firearms, and conclude that such a ban would most likely be constitutionally permissible. Following this conclusion, I will highlight the problems of enforcing such a ban. Lawmakers who are considering limiting or banning 3D printed firearms should strive to regulate this technology in a way that will promote the safety of firearm users and the public without imposing too many burdens on the continuing development of this new technology.

Part I of this Paper will briefly survey the rise of 3D printing technology, paying specific attention to the development of 3D printed firearms. Part II will summarize the current state of Second Amendment law, focusing primarily on the Supreme Court's decisions in *District of Columbia v. Heller* and *McDonald v. City of Chicago*, and the lower courts' following treatment of Second Amendment challenges to restrictions on firearms. Part III contains the bulk of my analysis. Here, I will contemplate a complete ban on 3D printed firearms. I will explore whether this ban would fall into any categories of traditional firearm regulation, the government's interests in enacting such a ban, and the different levels of scrutiny courts may apply to this type

[6] 130 S. Ct. 3020 (2010).

of ban. I will conclude that it very likely that courts would uphold a complete ban on 3D printed firearms. In Part IV, I will explore the difficulty of enforcing a restriction on 3D printed firearms and suggest several strategies for effective regulation, as well as several approaches that governments should avoid. In Part V, I conclude that while the Second Amendment will probably not be a substantial problem for restrictions on 3D printed firearms, significant questions about the practicality of these restrictions remain.

I. THE RISE OF 3D PRINTING

3D printing has captured the public's attention and imagination. *The Economist* contends that 3D printing marks a "third industrial revolution" that will be characterized by the merger of digital communication and efficiency with the physical manufacture of goods.[7] Others admit that while 3D printers may not change the world on their own, they will likely have a major impact on how items are manufactured.[8] Legal writers are also beginning to take note of the issues 3D printing may raise, with commentators noting the technology's influence in fields of intellectual property,[9] product liability,[10] and the Fourth Amendment.[11]

---

[7] *A Third Industrial Revolution*, ECONOMIST (Apr. 21, 2012), *available at* http://www.economist.com/node/21552901.

[8] Peter Day, *3D Printing: A Force for Revolutionary Change*, BBC (May 21, 2013), http://www.bbc.co.uk/news/business-22559022; *see also* Jim Chalmers, *3D Printing: Not Yet a New Industrial Revolution, But Its Impact Will Be Huge*, GUARDIAN (Dec. 10, 2013, 5:36 PM), http://www.theguardian.com/commentisfree/2013/dec/11/3d-printing-not-yet-a-new-industrial-revolution-but-its-impact-will-be-huge.

[9] Deven R. Desai & Gerard N. Magliocca, *Patents, Meet Napster: 3D Printing and the Digitization of Things*, 102 GEORGETOWN L. J., Forthcoming, 2014, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2338067.

[10] Nora Freeman Engstrom, *3-D Printing and Product Liability: Identifying the Obstacles*, 162 U. PA. L. REV. ONLINE 35 (2013).

[11] Julian J. Johnson, Note, *Print, Lock, and Load: 3-D Printers, Creation of Guns, and the Potential Threat to Fourth Amendment Rights*, 2013 ILL. J. TECH. L. & POL. 337 (2013).

A. 3D Printing Technology: A Brief Background

3D printers are machines that convert digital "blueprints" of objects into physical objects by building the physical versions "layer-by-layer."[12] A user downloads or creates a digital blueprint of some object, often created using a computer aided design (CAD) program.[13] Websites like Thingiverse offer users the opportunity to search for and download blueprints of objects that they wish to print.[14] Users can also upload their own designs to these websites so that others may view and download them.[15]

Once a user has downloaded a digital blueprint to his or her computer, the user then connects the computer to a 3D printer. After sending the blueprint to the printer, the printer "spreads thin layers of plastic or metal powder on top of each other" and then welds these layers together, ultimately creating a physical replica of the digital input.[16] Because of the precise scale on which these printers operate, 3D printers can "create objects with internal, movable parts.[17]

Users can purchase a 3D printer directly from 3D printer manufacturers such as Makerbot. Other retailers are beginning to carry 3D printers as well – for example, Staples is now selling the Cube brand of 3D printers.[18] The range of prices for 3D printers varies

---

[12] Michael Weinberg, *It Will be Awesome if They Don't Screw It Up: 3D Printing, Intellectual Property, and the Fight Over the Next Great Disruptive Technology*, PUBLIC KNOWLEDGE 2 (Nov. 2010), http://publicknowledge.org/files/docs/3DPrintingPaperPublicKnowledge.pdf.

[13] *Id.*

[14] *See MakerBot Thingiverse*, THINGIVERSE, http://www.thingiverse.com/about (last accessed January 30, 2014).

[15] *Id.*

[16] Day, *supra* note 8.

[17] Weinberg, *supra* note 12, at 2.

[18] *See Cube 3D Printers*, STAPLES, http://www.staples.com/Cube-3D-Printers/product_SS2044291 (last accessed January 30, 2014) (selling Cube 3D printers for "as low as $1,299.99").

depending on the size and range of materials the printer can process. The Makerbot line of 3D printers varies in price from $1,375.00 for its forthcoming 12.5-inch tall[19] 3D printer, to $6,499.00 for its forthcoming, 18-inch tall[20] "Z18" printer.

Most printers that are designed for general use by the public print objects made out of various types of plastics, while printers that are able to print metal components are generally far more expensive.[21] But 3D printing technology is a rapidly evolving industry, and prices are projected to fall as the technology becomes more advanced and popular.[22] Some commentators argue that enthusiasm and worries about 3D printing is misplaced, as printers are expensive, slow, and prone to errors.[23] But proponents of the technology point out that overcoming these barriers is only a matter of time, analogizing today's 3D printing industry to the early stages of computer development in the 1990s.[24]

---

[19] *Makerbot Replicator Mini Compact 3D Printer*, MAKERBOT, http://store.makerbot.com/replicator-mini (last accessed January 30, 2014).

[20] *Makerbot Replicator Z18 3D Printer*, MAKERBOT, http://store.makerbot.com/replicator-z18 (last accessed January 30, 2014).

[21] Doug Gross, *Texas Company Makes Metal Gun With 3-D Printer*, CNN (Nov. 8, 2013, 7:06 PM), http://www.cnn.com/2013/11/08/tech/innovation/3d-printed-metal-gun/.

[22] *See* Nick Bilton, *Disruptions: The 3-D Printing Free-For-All*, N.Y. TIMES BITS (Nov. 13, 2011, 2:17 PM), http://bits.blogs.nytimes.com/2011/11/13/disruptions-the-3-d-printing-free-for-all/. Prices are already much lower now than even a year or two earlier – with some printers selling for $500.00. *See* Rich Brown, *You Don't Bring a 3D Printer to a Gun Fight—Yet*, CNET (Sept. 6, 2012, 4:00 AM), http://news.cnet.com/8301-11386_3-57499326-76/you-dont-bring-a-3d-printer-to-a-gun-fight-yet/.

[23] *See* Charles W. Finocchiaro, Note, *Personal Factory or Catalyst for Piracy?: The Hype, Hysteria, and Hard Realities of Consumer 3-D Printing*, 31 CARDOZO ARTS & ENT. L.J. 473, 489-90 (2013). For illustrations of 3D printer errors, see *3D Printing Failures Shared Online*, BBC, (Aug. 17, 2013, 8:29 PM) http://www.bbc.co.uk/news/technology-23727229.

[24] *See* Weinberg, *supra* note 12, at 4.

B. The Creation, and Rapid Development, of 3D Printed Firearms

In May, 2013, the first firearm made entirely from 3D printed parts was successfully fired.[25] This firearm was called the "Liberator," and it confirmed that 3D printers could be used to print usable firearms.[26] The inventor of this firearm was Cody Wilson, a law student at the University of Texas, and founder of the non-profit organization, Defense Distributed.[27] Wilson's organization had already printed firearm parts – and had fired 600 rounds with an AR-15 assault rifle "with a 3D printed part . . . ."[28] The Liberator was printed from an $8,000.00, 3D printer, and the only non-printed component of the firearm was the firing pin, which was a nail.[29] Wilson included the metal firing pin in order for the gun to be visible to metal detectors, as a completely undetectable gun would be prohibited by federal law.[30]

Wilson's invention and firing of this 3D printed firearm was met by widespread media coverage and unease. The government ended up asking Defense Distributed to remove the blueprints for the Liberator from its website, but the design for the firearm had already been widely shared over the Internet.[31] Wilson's development of the Liberator signaled that even

---

[25] Greenberg, *supra* note 1.

[26] *Id.*

[27] *Id.*

[28] *'Pirate Bay' for 3D Printing Launched*, BBC (March 12, 2013, 1:55 PM), http://www.bbc.co.uk/news/technology-21754915.

[29] Adam Gabbatt, *Shots Fired From the World's First 3D-Printed Handgun*, GUARDIAN (May 6, 2013, 2:43 PM), http://www.theguardian.com/world/2013/may/06/3-handgun-fired-cody-wilson.

[30] *Id.* The law prohibiting firearms that are invisible to metal detectors is codified at 18 U.S.C. § 922(p).

[31] Charles C.W. Cooke, *There's No Stopping 3-D-Printed Guns*, NATIONAL REVIEW ONLINE (Nov. 11, 2013, 4:00 AM), http://www.nationalreview.com/article/363590/theres-no-stopping-3-d-printed-guns-charles-c-w-cooke.

printers that were capable of printing only plastic components could produce a working firearm.[32]

And these firearms did not even require an $8,000.00 investment to produce. Less than three weeks after Cody Wilson tested the Liberator, an engineer in Wisconsin used a $1,725.00 "Lulzbot" printer to make a pistol that successfully fired nine shots.[33] This signaled that firearms were effectively within reach of anybody with a working 3D printer and a firearm blueprint.

3D printed firearms did not remain constrained to the realm of plastic. Soon, another company, Solid Concepts, produced an all-metal firearm using a 3D printer.[34] Solid Concepts announced that the firearm had successfully fired over fifty rounds, and posted a video of the firearm in action.[35] This was a marked improvement over Wilson's Liberator, which had misfired at one point during Wilson's demonstration, and exploded after several more shots.[36] Solid Concepts was quick to point out that its firearm could not be manufactured using standard, desktop 3D printing technology.[37] But metal printers are evolving alongside regular 3D printers, and their price is also projected to fall.[38] Other 3D printing enthusiasts have created what appear to be working revolvers,[39] although whether these firearms can withstand sustained use is a

---

[32] *Id.*

[33] Greenberg, *supra* note 2.

[34] Alyssa Parkinson, *World's First 3D Printed Metal Gun*, SOLID CONCEPTS BLOG (Nov. 7, 2013, 12:00 PM), http://blog.solidconcepts.com/industry-highlights/worlds-first-3d-printed-metal-gun/.

[35] *See id.*

[36] Greenberg, *supra* note 1.

[37] Alyssa, *supra* note 34.

[38] *See* RT, *Home-Made Browning: 3D Printers Stoke Fears of Backyard Technology Explosion*, YOUTUBE (Nov. 28, 2013), http://www.youtube.com/watch?v=_EXsAeJ7RsU.

matter of debate.[40] However effective the gun may have been, its designer was arrested and sentenced to two years in prison for violating Japan's "strict gun laws."[41] And some developers have produced 3D printed bullets – although it seems that the printed component of the bullet is limited to the slug that is fired (since users are unable to print gunpowder).[42]

Meanwhile, 3D printed firearm designs were making advances in the digital context. Cody Wilson had already developed Defcad, a search engine for 3D printed parts, before the first test-firing of the Liberator pistol.[43] Users can search this website for various designs, including what seems to be a working, 3D printed revolver.[44] Encryption technology for 3D printing designs has also progressed, and users are now capable of scrambling the images of designs they share online.[45] This technology can be used by individuals who wish to hide contraband items, including firearms, from detection by authorities.[46]

---

[39] *See*, *infra*, note 44.

[40] John LaRocco, *Simulated Testing of a 3D Printed Revolver Cylinder*, PEEREVALUATION (2013), *available at* http://peerevaluation.org/data/f410588e48dc83f2822a880a68f78923/PE_doc_29812.pdf.

[41] Brian Krassenstein, *Two Year Sentence Handed Down to Yoshitomo Imura in Japanese 3D Printed Gun Case*, 3DPRINT.COM (Oct. 20, 2014) http://3dprint.com/20019/sentence-imura-3d-printed-gun/.

[42] *See* Fidel Martinez, *Bullets Join the 3-D Printed Arsenal*, THE DAILY DOT (May 24, 2013), http://www.dailydot.com/news/3d-printed-bullets-fired/.

[43] *'Pirate Bay' for 3D Printing*, *supra* note 28.

[44] *See Caliber Zig Zag Revolver Tank Gan Mk.*, DEFCAD, https://defcad.com/cad_objects/caliber-zig-zag-revolver-tank-gan-mk. While it is not immediately apparent on Defcad's web page that the displayed product is a working revolver, the page links to a YouTube video of the weapon being fired. *See* imura2011, *3D Printed Revolver First in the World Prototype Test Shooting*, YOUTUBE (Nov. 19, 2013), http://www.youtube.com/watch?v=HubsiAZSasA.

[45] Andy Greenberg, *3D-Printing 'Encryption' App Hides Contraband Objects In Plain Sight*, FORBES (Nov. 4, 2013, 9:38 AM), http://www.forbes.com/sites/andygreenberg/2013/11/04/3d-printing-encryption-app-hides-contraband-objects-in-plain-sight/.

[46] *Id.*

While 3D printing technology may be expensive and inefficient in its current stages, the technology is clearly capable of producing firearms. Working (albeit, unreliable) firearms can be produced using readily available printers that print plastic components, and more effective firearms can be produced by advanced printers that can print metal components. The massive strides that have been made in the past year alone indicate that 3D printed firearms will likely continue to develop, and the technology's current unreliability and inaccessibility may soon be overcome.

II. THE SECOND AMENDMENT BACKGROUND

While the Second Amendment has attracted the attention of legal commentators for some time, the Second Amendment as an individual right was largely constrained to the realm of scholarly commentary before the Supreme Court's decision in *District of Columbia v. Heller*.[47] While *Heller* clarified that the Second Amendment protects an individual right to bear arms, it left the extent of this protection unclear – meaning that lower courts have had to determine the permissibility of laws and regulations that restrict the possession of firearms. This Part explores *Heller* and its aftermath, and summarizes some of the lower court trends and developments following the *Heller* decision.

A. District of Columbia v. Heller

In 2008, the Supreme Court held, in *District of Columbia v. Heller*,[48] that the District of Columbia's ban on handgun possession in the home violated the Second Amendment right to keep and bear arms.[49] It had been almost 70 years since the Court had applied the Second

[47] 554 U.S. 570 (2008).

[48] 554 U.S. 570.

Amendment.[50] The Court's determination that the Second Amendment protected an individual, rather than a group, right to keep and bear arms, put an end to the debate over whether the amendment protected individuals at all.[51] The Court's ruling that the Second Amendment protected individual rights was soon incorporated against the states in *McDonald v. City of Chicago*.[52]

In *Heller*, the Court held that the Second Amendment protected an individual's right to keep a handgun in the home for purposes of self-defense.[53] The District of Columbia's handgun ban infringed on this right by prohibiting people from having working handguns readily available, and this type of ban violated the Second Amendment under any standard of scrutiny the Court might apply.[54] In reaching this strong conclusion about the protection of handguns in the home, the Court did not enunciate any standard of review for statutes that limited the ability of citizens to keep, carry, or purchase firearms.[55]

While the Supreme Court did not specify a standard of review for statutes restricting firearms, the Court did indicate that "longstanding regulations" were not threatened by its decision. Specifically, the Court noted:

---

[49] *Id.* at 622, 635.

[50] *See* Brannon P. Denning & Glenn H. Reynolds, *Five Takes on* McDonald v. Chicago, 26 J.L. & POL. 273, 274 (2011) (noting that the Supreme Court's "only real Second Amendment case of the twentieth century" was *United States v. Miller*, 307 U.S. 174 (1939)).

[51] *See*, WINKLER, *supra* note 5 at 106 – 13; Shalhope, *supra* note 5.

[52] 130 S. Ct. 3020, 3026 (2010).

[53] *Heller*, 554 U.S. at 592, 599.

[54] *Id.*

[55] *See McDonald*, 130 S. Ct. at 3105 (Stevens, J., dissenting); *see also* See Philip J. Cook et al., *Gun Control After* Heller*: Threats and Sideshows From a Social Welfare Perspective*, 56 UCLA L. REV. 1041, 1064 (2009).

> Nothing in our opinion should be taken to cast doubt on longstanding prohibitions on the possession of firearms by felons and the mentally ill, or laws forbidding the carrying of firearms in sensitive places such as schools and government buildings, or laws imposing conditions and qualifications on the commercial sale of arms.[56]

The Court reiterated this caveat in *McDonald* as well.[57]

While the Court did not enunciate a standard of scrutiny for constitutional review, there are several takeaways from these portions of the *Heller* opinion. The Court appeared to hold that a ban that prohibits the possession of firearms in the home for purposes of self-defense is unconstitutional under the Second Amendment. But firearms may still be regulated and restricted in ways that are consistent with longstanding regulations. So, presumably, even though a law banning felons from possessing firearms would prevent those felons from possessing firearms in their homes for self-defense, this sort of law would likely survive Second Amendment scrutiny, since the Court specifically indicated that this type of law is not threatened by its holding in *Heller*.[58]

B. Lower Court Decisions After Heller

Following *Heller*'s unclear discussion of Second Amendment rights, the lower courts were left to determine the scope of the Second Amendment's protection. But despite the failure of the Supreme Court to enunciate a standard of constitutional review for Second Amendment cases, lower courts have generally reached a consensus on how to determine when laws infringe people's Second Amendment rights.[59] While there have been several decisions that have struck

[56] *Heller*, 554 U.S. at 626–27.

[57] *See McDonald*, 130 S. Ct. at 3047.

[58] *See Heller*, 554 U.S. at 626–27.

[59] Nelson Lund, *Second Amendment Standards of Review in a* Heller *World*, 39 FORDHAM URB. L.J. 1617, 1622 (2012).

down laws as violating the Second Amendment, most decisions following *Heller* have upheld laws – particularly those laws that *Heller* indicated were "longstanding regulations."[60] Beyond these longstanding regulations, the level of scrutiny applied to laws restricting the right to bear arms for purposes of self-defense largely depends on the level of those laws' intrusion on the right.[61]

The Court's decision in *United States v. Masciandaro*[62] illustrates courts' attention to laws' level of intrusion on the right to bear arms for self-defense when determining what level of scrutiny to apply. In *Masciandaro*, the Fourth Circuit upheld a federal ban on the possession of loaded firearms in vehicles in national parks.[63] In upholding this ban, the court noted that the need to possess firearms for purposes of self-defense in national parks was less acute than it may otherwise be, as the parks are patrolled by U.S. park police.[64] Because the ban on loaded firearms in cars did not burden the "core" Second Amendment right to possess firearms in the home for self-defense, the court applied intermediate scrutiny, rather than strict scrutiny.[65] Accordingly, the government only needed to prove that the firearm restriction served an important government interest, and that the restriction was substantially tailored to achieve this interest.[66]

---

[60] *Id.*

[61] *Id.*

[62] 638 F.3d 458 (4th Cir. 2011).

[63] *Id.* at 474.

[64] *Id.*

[65] *Id.* at 469-71.

[66] *Id.*

Lower courts seem to agree that in many cases, an initial focus on a regulation's impact on the core right of law abiding citizens to self-defense in the home is required when it comes to determining whether a law violates the Second Amendment.[67] Alternatively, courts may seek to circumvent the decision on what level of scrutiny to apply and analogize a law to the "longstanding prohibitions" that *Heller* noted were not threatened by the Court's holding.[68] If a law infringes on the core right to self-defense, or substantially restricts law abiding individuals' ability to possess firearms for self-defense, then courts will apply a higher level of scrutiny than intermediate scrutiny.[69]

Under this framework for Second Amendment analysis, courts typically end up applying intermediate scrutiny to firearms restrictions. But strict scrutiny – which requires a compelling government interest, and that the law be narrowly tailored to achieve that interest[70] – is still relevant in discussions of firearm regulation. If a law ends up substantially restricting the core Second Amendment right to self-defense in the home, then the reviewing court must apply strict scrutiny. Moreover, some states grant stronger protections for the right to bear arms than the Second Amendment. For instance, Louisiana's constitution protects the individual right to bear

---

[67] *See, e.g.*, United States v. Mahin, 668 F.3d 119, 123 (4th Cir. 2012) (noting that intermediate scrutiny should be applied to firearms ban on citizens who do not follow the law because that these people fall outside of the Second Amendment's core protection); United States v. Marzzarella, 614 F.3d 85, 97 (3d Cir. 2010) (holding that a ban on firearms with obliterated serial numbers did not severely restrict the right to bear arms, and was therefore subject to intermediate scrutiny).

[68] *See, e.g.*, United States v. Yancey, 621 F.3d 681, 683-85 (7th Cir. 2010) (analogizing a prohibition on possession of firearms by those in possession of or addicted to controlled substances to the longstanding prohibition on firearm possession by felons).

[69] *See, e.g.*, Ezell v. City of Chicago, 651 F.3d 684, 708 (7th Cir. 2011) (noting that "a severe burden on the core Second Amendment right of armed self-defense will require an extremely strong public-interest justification and a close fit between the government's means and its end" and distinguishing this level of scrutiny from intermediate scrutiny).

[70] *See Marzzarella*, 614 F.3d at 96 & n.14 (defining strict scrutiny and rejecting it in the Second Amendment context).

arms, and goes on to require that any law restricting this right shall be subject to strict scrutiny.[71] Despite this strong language, the government may still overcome this level of scrutiny. Louisiana's ban on firearm possession by those on probation or parole survived strict scrutiny analysis.[72] Most recently, Louisiana's law restricting minors from possessing handguns survived strict scrutiny, with the Louisiana Supreme Court noting the tradition of the firearms ban and the immaturity of minors.[73]

III. APPLYING THE SECOND AMENDMENT TO A BAN ON 3D PRINTED FIREARMS

With this background on 3D printing and the Second Amendment in mind, this paper now turns to the question of the Second Amendment implications of restrictions on 3D printed firearms. Before getting to the analysis, however, a discussion of this section's framework is warranted.

In this section, I will be contemplating a complete ban on 3D printed firearms. This ban would contain two major parts: (1) a ban on the act of printing firearms,[74] and (2) a ban on possessing firearms that have been made through 3D printing. Of course, these outcomes might be achieved in a number of ways. For instance, a state may decide to ban the act of printing firearms by prohibiting the possession of digital blueprints for these firearms – which would

[71] LA. CONST. art. I, § 11.

[72] *See* State v. Draughter, 2013 WL 6474419 (La. 2013).

[73] State ex rel. J.M., 2014 WL 340999 at *1-2, *6-7 (La. 2014)

[74] The city of Philadelphia recently passed an ordinance that closely mirrors this proposal by banning the manufacture of firearms with a 3D printer by those who do not have a federal license to manufacture firearms. *See* Zenon Evans, *Philadelphia Becomes First City to Ban 3D-Printed Gun Manufacturing*, REASON.COM (Nov. 22, 2013, 4:23 PM), http://reason.com/blog/2013/11/22/philadelphia-becomes-first-city-to-ban-3.

make printing the firearms impossible. But for the sake of simplified analysis, I will focus on the two-part ban on printing and possessing 3D printed firearms.[75]

Because I ultimately seek to conclude that regulations on 3D printing will survive Second Amendment challenges, considering a complete ban on 3D printed firearms is particularly useful. Questions of constitutionality in the Second Amendment context often come down to whether a law significantly burdens the core Second Amendment right of possession of firearms for purposes of self-defense, and whether the law being considered is tailored substantially or narrowly to achieve the purpose of the law.[76] A complete ban on 3D printed firearms would burden any relevant Second Amendments more than a partial ban, and the complete ban, by definition, is less narrowly tailored than a partial ban. The upshot is that if a complete ban on 3D printed firearms would survive Second Amendment challenges, then narrower bans will also be likely to survive Second Amendment challenges.

In framing my approach this way, I recognize that this type of ban would restrict the printing of firearms by both private individuals and large-scale companies. The printing and selling of firearms by larger, established companies may be more amenable to regulation – perhaps by giving specialized licenses to these companies. This is certainly something worth exploring when it comes to planning maximally-effective regulations, and it is something I will discuss in more detail later in this paper.[77] But for the present purposes of the Second Amendment argument, I will accept that a complete ban on 3D printed firearms will restrict

[75] And for the sake of simplified phrasing, when I refer to a "ban on 3D printed firearms," that phrase will encompass both restrictions described herein unless specified otherwise.

[76] *See supra*, Part II. B.

[77] *See infra* Part IV.

printing and possession of all 3D printed firearms – regardless of whether they are made on personal or industrial printers.[78]

Of course, when it comes to the question of how narrowly the law is tailored, there is the possibility that courts may conclude that laws are improperly tailored to achieve government interests because a law is underinclusive.[79] The Supreme Court has taken this approach in First Amendment cases, noting that if unprotected speech is selectively banned, this practice may still violate the First Amendment because the law may discriminate based on the viewpoints expressed in the unprotected speech.[80] While this concern may be relevant, I will not address it in this paper. No cases striking down laws on Second Amendment grounds have done so on the grounds that the laws are underinclusive. And laws that tend to restrict firearms more narrowly than blanket bans tend to narrow restrictions along the lines longstanding restrictions on firearms that *Heller* indicated were not threatened by its holding.[81]

With this approach in mind, I will approach the Second Amendment question by first exploring whether a ban on 3D printed firearm would fall under one of the "longstanding" restrictions on firearm that *Heller* mentioned. I will then explore whether a ban on 3D printed firearms would substantially burden the core Second Amendment right to possess firearms in the

---

[78] Accordingly, this law would likely be even stricter than the United Kingdom's approach, which outlaws the manufacturing, transfer, and possession of firearms made from printed components, because the United Kingdom has a licensing scheme in place that may permit some parties to do so. *See* Freya Berry, *Britain Updates Rules Banning 3D-Printer Guns*, REUTERS (Dec. 5, 2013, 3:22 PM), http://uk.reuters.com/article/2013/12/05/us-britain-guns-idUKBRE9B40OV20131205.

[79] A law may fail to be sufficiently tailored to achieve a government interest because it is over inclusive, meaning that the law restricts more behavior than is necessary to achieve that interest, or because the law is under inclusive, meaning that the law does not restrict enough behavior to achieve the government's interest.

[80] *See* R.A.V. v. St. Paul, 505 U.S. 377, 386-88 (1992).

[81] *See* Lund, *supra* note 59, at 1622 (noting that courts tend to uphold those regulations that *Heller* indicates are longstanding restrictions on firearm possession).

home for purposes for self-defense. Next, I will evaluate whether the ban on firearms would survive intermediate scrutiny. I will do this by exploring the government's interest behind a ban on 3D printed firearms and how an innovative approach by the government at this stage of the analysis would give the government strong arguments in favor of the constitutionality of bans on 3D printed firearms. This section will conclude with a brief note on applying strict scrutiny to the ban on 3D printed firearms.

A. Would a Ban on 3D Printed Firearms Fall Under a Longstanding Restriction?

As has already been mentioned, the *Heller* ruling was not without caveats. The Court noted that its decision would not cast doubt on a number of "longstanding" restrictions on firearms, including laws restricting firearm possession by felons and the mentally ill, restrictions on possessing firearms in sensitive places like schools and government property, and conditions on the commercial sales of firearms.[82] The Court noted that this list of "presumptively lawful regulatory measures" was not exhaustive.[83]

The Court also looked to history in order to determine what types of firearms restrictions existed at the time of the Second Amendment's adoption. The Court noted that "the majority of the 19th-century courts to consider the question held that prohibitions on carrying concealed weapons were lawful under the Second Amendment or state analogues."[84] And the Court pointed out "the historical tradition of prohibiting the carrying of 'dangerous and unusual weapons.'"[85]

[82] District of Columbia v. Heller, 554 U.S. 570, 626–27 (2008).

[83] *Id.* at 627, n.26.

[84] *Id.* at 626.

Governments seeking to ban 3D printed firearms may claim that a restriction on these weapons are necessary to maintain the efficacy of the "presumptively lawful regulatory measures" that *Heller* specified. 3D printed firearms – particularly those that can be printed on personal computers – may be far easier to obtain than traditional firearms. People who want to print a firearm simply must obtain a 3D printer and the raw material for printing, and download a blueprint of a firearm. Blueprints may typically be found on websites that specialize in distributing CAD files for 3D printers – but these files may just as easily be obtained from individual users who possess the files, or from websites where those other users may post the files.[86] If 3D printed firearms can be downloaded and printed by anybody with a 3D printer, then there is virtually nothing preventing students from printing out firearms in dormitories, or felons from printing out firearms. Governments may argue that banning 3D printed firearms is the only way to prevent longstanding restrictions on the possession of firearms from becoming meaningless.

Critics may argue that there is no longstanding prohibition on the manufacture of firearms for personal use, so the government would be mistaken to claim that a ban on 3D

---

[85] *Id.* at 627. The Court used this tradition to justify the federal ban on machineguns and short-barreled shotguns – a move that has drawn criticism from commentators who point out that those weapons are not in common use because they were outlawed well after the adoption of the Second Amendment. *See* Adam Winkler, Heller*'s Catch-22*, 56 UCLA L. REV. 1551, 1560-61 (2009). While these arguments may be correct, I will not address them in this paper, as the fact remains that *Heller* indicated that prohibitions on dangerous and unusual weapons are apparently lawful, and this is the authority that will govern lower court decisions on the issue.

[86] *See* Liz Klimas, *3-D Printed Gun Designs 'Gone Dark': Wiki-Weapons Project Removes Designs After Gov't 'Claims Control of the Information'*, BLAZE (May 9, 2013, 11:55 PM), http://www.theblaze.com/stories/2013/05/09/3d-printed-gun-designs-gone-dark-wiki-weapons-project-removes-designs-from-web-at-govt-request/ (reporting that even after the government requested the removal of 3D printed firearm blueprints from Defcad, the files were still available on other websites, including Pirate Bay, "one of the largest bit torrent sites on the Web").

printing would fall into the category of longstanding restrictions.[87] But this is not what the government is arguing. The government's argument is that there are several longstanding restrictions on firearms that are very likely to be found constitutional under *Heller*. And if 3D printing continues to make technological advances and become more mainstream, restricting 3D printed firearms may be the only way for the longstanding restrictions to remain meaningful.

The Government may also argue that 3D printed firearms fall into the category of "dangerous and unusual firearms," the carrying of which has been historically prohibited.[88] 3D printed firearms, as a new technological development, are unusual. Moreover, these firearms can be uniquely dangerous, since they may be printed from undetectable plastic and produced in sensitive locations that happen to have 3D printers available.

Critics may point out that 3D printed firearms – especially those that are made on personal printers – tend to be less powerful and reliable than existing firearms.[89] Because of this, those 3D printed firearms that prompt the most concern – the ones printed from personal machines – are not uniquely dangerous under the Court's meaning in *Heller*.[90] They may, in fact, be "about as likely to kill the gunman as the target."[91]

---

[87] *See* Peter Jensen-Haxel, Comment, *3D Printers, Obsolete Firearm Supply Controls, and the Right to Build Self-Defense Weapons Under* Heller, 42 GOLDEN GATE U.L. REV. 447, 479 (2012).

[88] Heller, 554 U.S. at 627; *see also* WILLIAM BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND: IN FOUR BOOKS; WITH AN ANALYSIS OF THE WORK, VOLUME 4 *148-49 ("The offense of *riding* or *going armed* with dangerous or unusual weapons is a crime against the public peace").

[89] *See* Henry Fountain, *Tools of Modern Gun Making: Plastic and a 3-D Printer*, N.Y. TIMES (Jan. 29, 2013) http://www.nytimes.com/2013/01/30/science/surprising-tools-of-modern-gunmaking-plastic-and-a-3-d-printer.html?_r=0.

[90] Jensen-Haxel, *supra* note 87, at 489-92.

[91] Fountain, *supra* note 89.

While 3D firearms produced by personal printers may not be as strong or reliable as normal firearms, the ease with which they can be concealed from metal detecting technology may make them uniquely dangerous. Federal law prohibits the manufacture and possession of firearms that cannot be detected by walk-through metal detectors "after removal of grips, stocks, and magazines."[92] As Cody Wilson illustrated with the Liberator, 3D printed firearms may be produced that are entirely made from plastic – the one metal component of the Liberator was included in the design simply to ensure compliance with federal law.[93] Governments may argue that 3D printed firearms are unusually dangerous because they can be easily made from undetectable materials, and banning 3D printed firearms is the only way to effectively restrict undetectable firearms.

Admittedly, many of these arguments do not apply to 3D printed firearms that are made from metal, meaning that critics of bans on 3D printed firearms can argue that the bans would be overbroad. Users who have advanced printers that can produce metal firearms would not fall into the category of producing unusually dangerous weapons – as these firearms would be just as detectable as traditional firearms. Moreover, 3D printers that are capable of printing metal firearms are often very expensive and belong to large companies that would likely produce firearms for sale, rather than personal use.[94] The upshot of this is that bans that seek to cleanly rely on longstanding restrictions on firearms may need to be restricted to personal 3D printers.

---

[92] 18 U.S.C. § 922(p)(1)(A) (2014).

[93] *See* Gabbatt, *supra* note 29.

[94] *See* David Szondy, *Solid Concepts Manufactures First 3D-Printed Metal Pistol*, GIZMAG (Nov. 8, 2013), http://www.gizmag.com/worlds-first-3d-printed-gun/29702/ ("The printers used [to produce a metal firearm] weren't the desktop sort using plastic filaments, but industrial printers that require expert handing and cost many thousands of dollars").

B. 3D Printed Firearms Bans and Substantial Burdens on the Right to Bear Arms

Setting aside questions of longstanding restrictions, the first question courts will consider in evaluating the constitutionality of a ban on 3D printed firearms is whether the ban is a substantial burden on the core Second Amendment right. The general consensus of the courts is that the Second Amendment protects the core right of law-abiding citizens to engage in self-defense when in the home.[95]

If courts conclude that a ban on 3D printed guns would not substantially burden the core Second Amendment right, then the law would need to survive intermediate scrutiny – meaning the government would need to prove that it has an important interest, and that the ban on 3D printed firearms is substantially tailored to achieve that interest.[96] But if the court concludes that a ban on 3D printed firearms substantially burdens the core Second Amendment right, then the ban will probably have to survive strict scrutiny, or something close to strict scrutiny.[97] If the court applies strict scrutiny, then the government would need to prove that it has a compelling interest and that the ban is narrowly tailored to achieve this interest.[98]

The government has a strong argument that a ban on 3D printed firearms does not put a substantial burden on the right to bear arms for purposes of self-defense in the home. Even if the government completely bans 3D printed firearms, people can still purchase and own traditional firearms. So while one extra option for defending oneself in the home may be foreclosed by a

[95] *See* United States v. Mahin, 668 F.3d 119, 123 (4th Cir. 2012); *see* United States v. Masciandaro 638 F.3d 458 (4th Cir. 2011); *see generally* Lund, *supra* note 59, at 1622.

[96] *Masciandaro*, 638 F.3d at 469-71.

[97] *See* Ezell v. City of Chicago, 651 F.3d 684, 708 (7th Cir. 2011) (while the court did not apply strict scrutiny to a law that burdened the core Second Amendment right, it applied a higher standard of scrutiny than intermediate scrutiny in striking down the ban).

[98] *See* United States v. Marzzarella, 614 F.3d 85, 96 & n.14 (3d Cir. 2010) (defining strict scrutiny and rejecting it in the Second Amendment context).

ban on 3D printing, this loss of an option is far from a loss of the ability to defend oneself in the home.

Peter Jensen-Haxel raises an interesting point that people who are disabled may require customized firearms in order to defend themselves in their homes, and that banning 3D printed firearms could interfere with this ability.[99] While Jensen-Haxel's claim that his argument is supported by longstanding common law is strained,[100] critics of a ban on 3D firearms may claim that a total ban on these firearms substantially burdens the core Second Amendment rights of those who may be unable to use traditional firearms.

The government may reply that while individuals with disabilities may be burdened by a ban on 3D printed firearms, the burden on this particular group does not necessarily mean that a law banning 3D printed firearms substantially burdens core Second Amendment rights. The class of individuals who would be detrimentally affected is small – limited to those who with disabilities – but not with disabilities so severe that they could not defend themselves even with access to 3D printed firearms. The small size of the group may lead courts to conclude that the infringement of the law on Second Amendment rights is not substantial.

Josh Blackman argues that the Second Amendment protects a right to make firearms, and notes that making firearms has traditionally been subjected to far less regulation than purchasing firearms.[101] Blackman notes that people have made their own firearms since the time of the

---

[99] Jensen-Haxel, *supra* note 87, at 481.

[100] Jensen-Haxel attempts to draw support from William Blackstone's commentaries by pointing out that Blackstone "explained that limbs threatened with debilitating injury could be defended with deadly force, even if life was not threatened, precisely because loss of their function meant privation of self-defense." *Id.* While Blackstone's point is a notable illustration of the strength of the right to self-defense, the selection that Jensen-Haxel cites say nothing about the rights of those who are already disabled.

[101] Josh Blackman, *The 1st Amendment, 2nd Amendment, and 3D Printed Guns*, 81 TENN. L. REV. 479, 496-97 (2014).

American Revolution and that the ability to make one's own firearms gives people the ability to make guns that are customized to their self-defense needs.[102] Blackman concludes that restrictions on making firearms therefore do not fall under any "longstanding" restriction on the right to keep and bear arms.[103] He also concludes that a ban on making personalized firearms would not survive Second Amendment review, even if people could purchase firearms.[104]

While people have indeed been making their own firearms for some time, and while people may make firearms that are more suited to their individualized wants or needs, Blackman's prediction that a ban on the ability to make one's own guns would be unconstitutional is by no means guaranteed. The *Heller* Court indeed noted that "longstanding" restrictions on the right to possess firearms were not affected by the ruling.[105] This point that exceptions may exist to Second Amendment protections in the case of longstanding restrictions does not imply that a longstanding *lack* of restrictions gives rise to Second Amendment protections.

Moreover, it is not clear why a prohibition on making one's own firearms would violate the Second Amendment, since people could still purchase firearms from gun manufacturers. Blackman contends that a prohibition on making one's own guns would "not be narrowly-tailored enough to survive review" without "a showing of an important state interest."[106] First, this argument is nonsensical, since a law implicating constitutional scrutiny must have both a sufficiently strong government interest in which it is based *and* be sufficiently tailored to achieve

---

[102] *Id.*

[103] *Id.* at 497.

[104] *Id.*

[105] District of Columbia v. Heller, 554 U.S. 570, 626–27 (2008).

[106] Blackman, *supra* note 100, at 497.

that interest without imposing overly broad restrictions on the constitutional right.[107] A law that is insufficiently tailored does not become sufficiently tailored if the government's interest is sufficiently strong, since those are two independent steps of the constitutionality analysis. Second, Blackman does not provide any reason why people's ability to purchase firearms would not allow them to fulfill their self-defense needs in the absence of the ability to make their own firearms. Even if people cannot make their own guns, they may still purchase pre-made firearms from gun manufacturers. It is not clear why restricting people's ability to make their own guns when they still have the ability to buy guns is an overly broad restriction on Second Amendment protections.

Finally, even if a law prohibiting people from making their own firearms would violate the Second Amendment, it does not follow that a law banning 3D printed guns would violate the Second Amendment, since people could make guns by means other than 3D printing. And as Blackman admits, these guns are arguably safer and more effective than 3D printed guns.[108]

Because people would still have constitutionally-protected access to traditional firearms, a government ban on 3D printed firearms would probably not substantially burden the right to self-defense in the home. In *Heller*, the Court noted that a handgun may be preferred to alternative long guns in a self-defense situation – handguns may be easier to store and access, they are easier to lift, and people can hold a handgun in one hand while calling the police with the other.[109] All of these benefits of handguns remain if the government bans 3D printed firearms – people simply need to purchase traditional firearms instead of printing firearms. If courts conclude that a ban on 3D printed firearms does not substantially burden the core Second

---

[107] *See*, *infra*, Part III. C (describing intermediate scrutiny).
[108] Blackman, *supra* note 100, at 487-88.

[109] *Heller*, 554 U.S. at 629.

Amendment right to self-defense in the home, the government must then show that a ban on 3D printed firearms passes intermediate scrutiny.

C. Subjecting a Ban on 3D Printed Firearms to Intermediate Scrutiny

A law or regulation passes intermediate scrutiny if the government enacting the law has an important interest and if the law is substantially tailored to achieve that interest.[110] Intermediate scrutiny, while a more stringent standard than rational basis scrutiny, has not been a very difficult obstacle for laws restricting the possession of firearms.[111] In intermediate scrutiny review, two questions need to be addressed: (1) whether the government has an important interest behind banning 3D printed firearms and, (2) whether banning 3D printed firearms is substantially tailored to that interest.

1. The Government's Interests in Banning 3D Printed Firearms

The government may argue that it has an interest in protecting public safety. This is an interest that is commonly invoked when regulations restricting firearms are challenged on Second Amendment grounds, and courts tend to conclude that it is an important interest.[112] Specifically, the government may argue that it has an interest in protecting the safety of members of the public who may be injured by somebody with a 3D printed firearm.

3D printing may involve other interests the government may invoke, however, and it would be strategic for the government to point out a variety of interests driving any ban on 3D

---

[110] *See, e.g.*, United States v. Reese, 627 F.3d 792, 802 (10th Cir. 2010); United States v. Marzzarella, 614 F.3d 85, 97 (3d Cir. 2010).

[111] *See, e.g.*, United States v. Skoien, 614 F.3d 638, 646–47 (7th Cir. 2010) (en banc) (Sykes, J., dissenting) (noting that the majority was taking a lenient approach to a law when applying intermediate scrutiny).

[112] *See, e.g.*, United States v. Masciandaro, 638 F.3d 458, 473 (4th Cir. 2011) (holding that a government's interest in protecting public safety is sufficient under an intermediate scrutiny standard of review); *Skoien*, 614 F.3d at 642 ("no one doubts that the goal of . . . preventing armed mayhem, is an important governmental objective").

printed firearms. In particular, the government may want to emphasize that it is concerned with the safety of the firearms *user* – in addition to members of the general public – because of the risks associated with 3D printed firearms. Currently, 3D printed firearms that are produced using personal printers are criticized as being unreliable, and are prone to malfunction or even explode.[113] If users mistakenly print firearms using the wrong type of plastic, the firearm may end up misfiring or exploding, causing serious injuries.[114]

Beyond the printing and assembly of firearms, users may face a danger of harm from the electronic aspect of 3D printing. In order to print anything on a 3D printer, users must first develop or download a digital blueprint of the object they would like to print. Digital blueprints are available for download on specialized websites like Thingiverse, but may also be uploaded onto private websites, or emailed between individuals. If 3D printing blueprints become more widespread, it is possible that unreliable blueprints may proliferate, leading to the printing of unreliable firearms. The security firm, Symantec, has predicted that blueprints for 3D printers will be a target for cybercriminals as the technology becomes more mainstream, and the government may argue that restricting 3D printed firearms may be the only way to prevent attacks in cyberspace from causing physical injury arising from printed weapons.[115] Focusing on the digital vulnerability of 3D printed firearms is particularly strategic because the danger of

---

[113] *See* Greenberg, *supra* note 1.

[114] *See* Andy Greenberg, *3D-Printed Gun Stands Up to Federal Agents' Testfiring—Except When it Explodes (Video)*, FORBES (Nov. 14, 2013, 11:41 AM), http://www.forbes.com/sites/andygreenberg/2013/11/14/3d-printed-gun-stands-up-to-federal-agents-testfiring-except-when-it-explodes-video/ (Reporting that a 3D printed firearm made out of a particular plastic, VisiJet, exploded as soon as it was fired).

[115] *See* Divina Paredes, *Symantec: Global Training Programme in Cyber Security to be Piloted in New Zealand and Australia*, CIO (Nov. 30, 2013, 6:00 AM), http://www.cio.co.nz/article/533150/symantec_global_training_programme_cyber_security_piloted_new_zealand_australia/.

cyber-attack will remain, even as 3D printing technology improves, and as personally-printed firearms become more reliable.

In advancing arguments about its interest, the government should emphasize both the danger 3D printed firearms may pose to the public-at-large, and to firearm users. By structuring its interest arguments this way, the government will have more options available when it comes to defending how specifically the law is tailored.

2. Whether a Ban on 3D Printed Firearms is Substantially Related to Government Interests

Courts must also evaluate whether a ban on 3D printed firearms is substantially related to the government's interests motivating the ban. While this test is more demanding than the rational basis test, which examines whether a law is "rationally related" to the government interest behind the law, courts may still be lenient in concluding that a law is substantially related to a government interest.

In *United States v. Skoien*, an en banc Seventh Circuit upheld the defendant's conviction for violating a federal law banning the possession of firearms by those who have been convicted of misdemeanor domestic violence.[116] Following the government's concession that a standard of intermediate scrutiny should be applied to the law, the court concluded that "[b]oth logic and data establish a substantial relation between § 922(g)(9) and this objective."[117] The court noted that people who commit misdemeanor domestic violence tend to reoffend, and that firearms are more dangerous than other weapons in domestic disputes.[118] The dissent pointed out that the court was particularly lenient when it came to the government's burden to prove a substantial

[116] 614 F.3d 638, 639, 645 (7th Cir. 2010) (en banc). The statute at issue was 18 U.S.C. § 922(g)(9) (2006).

[117] *Skoien*, 614 F.3d at 641-42.

[118] *Id.* at 633-34.

connection between the law and the government's interest in preventing armed mayhem, and warned that the court's understanding of the evidence may be mistaken.[119] *Skoien* illustrates that while governments must prove something more than a rational connection between the law and the government interest, there is room for leeway when it comes to determining whether a law is substantially tailored to meet that interest.

With this in mind, governments that seek to pass laws banning 3D printed firearms have a strong argument that the laws are substantially tailored to achieve government interests. As far as the government's interest in public safety is concerned, the government can point out that users can print out firearms anywhere, as long as a 3D printer is present in that location. These locations could include *Heller*'s sensitive locations, including government property and schools. These locations are sensitive because a firearm there may present a particular threat to other people or to government officials. Moreover, the government can argue that the ease with which people can print plastic firearms using 3D printers makes it more likely that people can print firearms that can avoid detection by metal detectors.[120]

People challenging the ban on 3D printed firearms can respond that a complete ban is overbroad. The government could (and the federal government already does) ban firearms that cannot be detected by metal detectors.[121] This law would make it illegal to carry firearms made entirely from plastic, so a separate ban on 3D printed firearms would not meaningfully contribute to the elimination of undetectable firearms. And laws could be passed that restrict the location of 3D printers, which would keep them out of sensitive locations, which would keep printed

[119] *Id.* at 651-52 (Sykes, J. dissenting).

[120] *See* Jana Winter, *Homeland Security Bulletin Warns 3D-Printed Guns May be 'Impossible' to Stop*, FOX NEWS (May 23, 2013), http://www.foxnews.com/us/2013/05/23/govt-memo-warns-3d-printed-guns-may-be-impossible-to-stop/.

[121] *See* 18 U.S.C. § 922(p)(1)(A) (2006).

firearms out of those locations rather than banning them entirely. While these arguments might not be enough to convince a court that a law banning 3D printed firearms is not substantially tailored, they may, at least, make the government's job harder when it comes to arguing for the constitutionality of the law.

The government could bolster its position by pointing to its interest in protecting the users of firearms. The government can point to the unreliability of firearms that are printed by personal 3D printers and argue that users of these firearms would be at a high risk of harm because these firearms may misfire or explode. Moreover, the government can argue that 3D printed firearms need to be prohibited because of the danger of flawed or hacked blueprints for these firearms. Unsuspecting users might download a compromised blueprint that produces a useless firearm, or worse, produces a firearm that is even more likely to explode. These arguments for substantial tailoring based on user safety may be more convincing than arguments concerning general public safety because the dangers that 3D printed firearms pose to their users are largely unique to the printed firearms – particularly the concerns of flawed digital blueprints.

Admittedly, challengers of a ban on 3D printed firearms can push back by arguing that there are some 3D printed firearms that are reliable. Would-be purchasers from industrial-scale producers of printed, metal firearms can argue that these firearms are safer than personally-printed firearms.[122] These challengers may also argue that a complete ban on 3D printed firearms is overbroad because it would prohibit the possession of metal firearms that happened to be printed, rather than made traditionally, by industrial producers.

While these challenges may have merit, it is unlikely that they would rise to the level of disproving a substantial connection between the ban on 3D printed firearms and the

[122] *Compare* Alyssa, *supra* note 34 (announcing that Solid Concepts' printed firearm had fired 50 shots) *with* Greenberg, *supra* note 1 (noting that the plastic Liberator pistol had exploded after several shots).

government's interest in user and public safety. Solid Concepts, the makers of the first 3D printed metal firearm, noted that the firearm was not for mass consumption.[123] And this stance is not surprising. While industrial 3D printers are particularly suited for printing prototypes of new products or parts, traditional manufacturing still tends to be more cost-effective when it comes to the mass production of goods.[124] If reliable, printed firearms are not widely available, restricting them will not meaningfully undermine the government's arguments that the law is substantially related to protecting user safety.

The government has a strong argument that prohibiting 3D printed firearms is substantially related to its interest in protecting public safety. And the government may avoid the most obvious problems with this argument by emphasizing the additional interest in protecting the safety of firearms users. Between these two interests, the government will probably be able to show that a complete ban on 3D printed firearms passes intermediate scrutiny.

D. A Brief Note on Strict Scrutiny

As argued in Part III.B, because a ban on 3D printed firearms does not substantially burden the right to bear arms, the government will probably only need to argue that a ban on 3D printed firearms passes intermediate scrutiny. But if courts come out differently on the substantial burden question, the government will probably need to argue that the ban on 3D printed firearms passes strict scrutiny, or something similar to it.[125] Additionally, my conclusion

---

[123] *See* RT, *supra* note 38.

[124] *See* BENJAMIN GRYNOL, DELOITTE, DISRUPTIVE MANUFACTURING: THE EFFECTS OF 3D PRINTING 6-7 (2013) *available at* http://www.deloitte.com/assets/Dcom-Canada/Local%20Assets/Documents/Insights/Innovative_Thinking/2013/ca_en_insights_disruptive_manufacturing_102813.pdf.

that the restriction will simply need to pass intermediate scrutiny does not apply to the state of Louisiana. Louisiana's constitution requires any restriction on the right to bear arms to pass strict scrutiny.[126]

To pass strict scrutiny, the government must show that its law is based on a compelling government interest and that the law is narrowly tailored to meet this interest.[127] A law that is subjected to strict scrutiny is unlikely to survive review, although it is not impossible.[128] In fact, a law prohibiting parolees and probationers from possessing firearms recently survived strict scrutiny review in the Louisiana Supreme Court.[129] But if courts end up applying strict scrutiny review, a law that completely bans 3D printed firearms is unlikely to survive.

IV. THE PROBLEM OF ENFORCEMENT AND EFFECTIVE REGULATION

The primary goal of this paper is to show that bans on 3D printed firearms will survive Second Amendment challenges. While my preceding arguments have shown that the Second Amendment will not be a significant obstacle to restrictions on these weapons, constitutional challenges may be the least of the government's worries. Digital blueprints for 3D printed firearms can be downloaded from websites and distributed between users. And these firearms

---

[125] *See* Lund, *supra* note 59, at 1622; *see also* Ezell v. City of Chicago, 651 F.3d 684, 708 (7th Cir. 2011) (noting that "a severe burden on the core Second Amendment right of armed self-defense will require an extremely strong public-interest justification and a close fit between the government's means and its end" and distinguishing this level of scrutiny from intermediate scrutiny).

[126] LA. CONST. art. I, § 11 ("The right of each citizen to keep and bear arms is fundamental and shall not be infringed. Any restriction on this right shall be subject to strict scrutiny").

[127] *See* United States v. Marzzarella, 614 F.3d 85, 96 & n.14 (3d Cir. 2010) (defining strict scrutiny and rejecting it in the Second Amendment context).

[128] *See* Adam Winkler, *Fatal in Theory and Strict in Fact: An Empirical Analysis of Strict Scrutiny in the Federal Courts*, 59 VAND. L. REV. 793, 795–96 (2006).

[129] *See* State v. Draughter, 2013 WL 6474419 (La. 2013).

can be printed from 3D printers, which anybody can purchase from specialized websites or major retailers. Even if the government bans 3D printed firearms, the law may do little to actually prevent the making and possession of these firearms.

An extended discussion of policy proposals that can assure effective enforcement is beyond the scope of this paper. But there are several approaches the government should consider taking, and several approaches that may be particularly problematic that I will discuss in this section. Ultimately, regulating and enforcing regulations on 3D printed firearms is a matter that many experts (with technical knowledge ranging beyond constitutional law) must discuss and develop.

A. Potential Approaches for Regulation

When regulating 3D printed firearms, it is important for the government to keep in mind that there are many actors involved. Deven Desai and Gerard Magliocca emphasize that "[t]here are several parts to the 3D printer environment," including design files stored on specialized repositories like Thingiverse, users who generate designs on their owns, Internet service providers, makers of raw materials that are put into 3D printers, 3D printer manufacturers, and the end users of the printers and design files.[130] This paper's subject so far has been a ban on the printing and possession of 3D printed firearms, but this ban would only affect one part of the 3D printing system – the end user.

In regulating 3D printed firearms, the government should contemplate all stages of the 3D printing process. Banning the printing and possession of 3D printed firearms creates a disincentive for the user to print and possess the firearm for fear of being caught. But the government could create incentives and disincentives at other stages of the process. One

[130] Desai & Magliocca, *supra* note 9 at 42-43.

extreme example might be to ban the distributions of the designs for 3D printed firearms, and to prosecute people who distribute these designs. Or, in lieu of criminal prosecution, governments could enact laws that provide for those distributing firearm designs to be held liable for any harm caused by their firearms.

An alternate, less disruptive approach, may be to enact regulations that control certain aspects of the 3D printing process without resorting to widespread criminal or civil liability. For example, Create it REAL, a manufacturer of 3D printers, has also "developed software that looks for the characteristics of weapon designs and, when detected, blocks the printer from making a firearm."[131] Governments might require companies that make 3D printers to develop and install similar software in their printers. This requirement would not interfere with the sale and use of 3D printers for non-firearm purposes. Even if users were able to obtain digital blueprints to print firearms, they would not be able to print from these blueprints.

Admittedly, users may try to work their way around these barriers through the use of encryption technology. For example, the program "Disarming Corruptor," allows the makers of digital blueprints to digitally scramble the appearance of their blueprints and selectively distribute the key for this encryption to specific users.[132] This can allow sellers or distributers of digital blueprints to transfer blueprints that may be illegal, or that may infringe on copyright protections (something the software's makers strongly imply – as a scrambled blueprint for a Mickey Mouse sculpture is one of the items included in their promotional video).[133] The Disarming Corruptor software does not appear capable of "fooling" printers – as users must

[131] Georgi Kantchev, *Authorities Worry 3-D Printers May Undermine Europe's Gun Laws*, N.Y. TIMES (Oct. 17, 2013), http://www.nytimes.com/2013/10/18/business/international/european-authorities-wary-of-3-d-guns-made-on-printers.html?ref=technology&_r=1&.

[132] *See* Greenberg, *supra* note 45.

[133] *Id.*

decrypt the files before printing them, meaning that the printer would still be printing from a non-encrypted blueprint. But this type of encryption technique indicates that attempts to install preventative software will require constant effort and upgrading. All may not be lost, however, since type of constant effort and upgrading may be something that quickly-evolving 3D printing companies can undertake.

Finally, governments should consider exceptions or licenses that may allow for the creation of 3D printed firearms by industrial printers. As companies like Solid Concept have shown, advanced 3D printers are capable of printing metal firearms that are of comparable durability and quality to traditional firearms.[134] But the printers required to manufacture these firearms are extremely expensive and likely to be owned only by large companies.[135] Governments should allow companies that use advanced 3D printers to apply for a license to print metal firearms. As I mentioned previously, even once the government has specified that its interest in banning 3D printed firearms is to prevent harm to the firearm user, the law is still overbroad because it would prohibit the manufacture of firearms by companies that employ advanced techniques to produce reliable, metal firearms. A licensing scheme for these companies would eliminate this overbreadth.

B. Regulations to Avoid

There are some restrictions relating to 3D printing that may make a ban on 3D printed firearms more effective, but these restrictions may have too negative of an impact on technological development. Alternatively, some restrictions that indirectly prevent the use of 3D

[134] *See*, Alyssa, *supra* note 34.

[135] *Id.*

printed firearms may veer dangerously close to creating a substantial restriction on people's right to possess firearms for purposes of self-defense, which could violate the Second Amendment.

Examples of laws that would unduly constrain technological development include laws outlawing the use of personal 3D printers, and, potentially, laws that would criminalize the distribution of digital blueprints for firearms. If the government outlaws personal 3D printers entirely, then this technology's potential will be stifled. And despite all of the concern these machines generate when it comes to the printing of firearms and weapons, 3D printers may be used for many other purposes.[136] Personal 3D printers are in a stage of rapid development, and banning them outright would greatly impede the potential positive consequences of this development. Moreover, even if they are not yet mainstream technology, 3D printers have become relatively popular, and are being sold by major retailers.[137] Because of this, an outright ban would probably be politically unpopular.

Governments that want to ban the dangers of undetectable, printable-anywhere firearms may seek to enact broader laws that would have an effect of reducing the danger caused by 3D printed guns. For example, a government may seek to place heightened restrictions on ammunition. Even if 3D printed firearms are difficult to detect and can be printed in sensitive places, they are not dangerous if they are not loaded, and ammunition may be easier to control through restrictions.

The problem with an approach like this would be that a restriction on ammunition, if effective enough to curtail the use of 3D printed firearms, would likely constitute a substantial burden on the core, Second Amendment right to self-defense in the home. While 3D printed

---

[136] *See, e.g.*, Stuart Dredge, *30 Things Being 3D Printed Right Now (And None of Them are Guns)*, GUARDIAN (Jan. 29, 2014, 7:40 AM), http://www.theguardian.com/technology/2014/jan/29/3d-printing-limbs-cars-selfies.

[137] *See Cube 3D Printers*, *supra* note 18.

firearms cannot be used for nefarious purposes without ammunition, traditional firearms cannot be used for self-defense without ammunition.

A strong restriction on ammunition would likely be held to be more restrictive of firearm use than Chicago's ban on gun ranges, which was held likely to be unconstitutional in *Ezell v. City of Chicago*.[138] There, the court held that the ban on firing ranges burdened citizens' abilities to engage in target practice, which was "an important corollary" to the right to bear arms in self-defense.[139] The court noted that Chicago required training with firearms before people could successfully obtain a firearms permit – which gave the court an "additional reason to closely scrutinize the range ban."[140] Because ammunition is required for firearms to function, the right to purchase and possess ammunition would also probably be found to be an important corollary to the right to bear arms in self-defense.

While there are certain approaches to regulation the government may take to ensure that a ban on 3D printed firearms is effective, governments must make sure that they do not stray too far in the direction of restricting the right to bear arms in self-defense. Moreover, governments must take heed of the potential of 3D printing, and try to mitigate damage to this quickly-evolving industry that strong restrictions could cause.

CONCLUSION

Restrictions on 3D printed firearms are likely to evoke strong opinions and resistance due to the inherently charged nature of political debate on firearms policy.[141] But even if

[138] *See* Ezell v. City of Chicago, 651 F.3d 684, 708-10 (7th Cir. 2011).

[139] *Id.* at 708.

[140] *Id.*

governments seeking to restrict these firearms meet political resistance, these bans would most likely survive Second Amendment challenges. Lower courts tend to recognize limits on the right to bear arms, and the availability of traditional firearms would mean that a restriction on 3D printed firearms would be very unlikely to significantly burden the core Second Amendment right.

But restricting 3D printed firearms is difficult, given the nature of 3D printing and the proliferation of digital designs. Governments seeking to effectively restrict 3D printed firearms will need to balance considerations of security, technological development, and constitutionality in enacting an effective set of restrictions. Balancing these factors will require careful attention to the impact of regulations and continuing developments in 3D printed technology. While this Paper proposes several initial policy considerations, there are certainly more that are being examined now, and more considerations that have yet to be realized.

[141] *See, e.g.*, Ana Marie Cox, *On 3D Guns, Congress Proves Yet Again How Scared it is of the Gun Lobby*, GUARDIAN (Dec. 11, 2013, 8:45 AM), http://www.theguardian.com/commentisfree/2013/dec/11/congress-3d-guns-scared-gun-lobby.

SYRACUSE JOURNAL OF SCIENCE & TECHNOLOGY LAW

VOLUME 31 2014-2015 ARTICLE 4, PAGE 98

PRIVACY EXPECTATIONS IN ONLINE VIDEO GAMES: IN LIGHT OF EDWARD SNOWDEN'S NSA DOCUMENT LEAK

Matthew Knopf

ABSTRACT

On December 9, 2013, the British Newspaper *The Guardian*, published documents from the National Security Administration provided by the whistleblower Edward Snowden. These documents revealed that surveillance agencies of the United States and United Kingdom governments were conducting intelligence operations in a search for terrorists inside of massive multiplayer online video games, such as *World of Warcraft* and *Second Life*. Online video game players live across the globe and within the United States and many of the computer servers on which video games operate are inside of the United States. The revelations of these documents lead to questions of whether there are any expectations of privacy for video game players and the communications between players within those video games. Violations of privacy could hinder player anonymity, a key component of certain types of online gaming that encourages escapism. Conversely, ending anonymity could encourage fairer and more civil discourse in the virtual gaming worlds. In the end, it is in the best interests of the gaming companies to continue to cooperate with governments in order to monitor and detect suspicious activity. It is most likely that gamers do not have an expectation of privacy in the virtual world.

INTRODUCTION

On December 9, 2013, the British Newspaper *The Guardian* published documents from the National Security Administration ("NSA documents") provided by the whistleblower Edward Snowden.[1] These documents revealed that surveillance agencies of the United States and United Kingdom governments were conducting intelligence operations in a search for terrorists inside of massive multiplayer online ("MMO") video games such as *World of Warcraft* and *Second Life*.[2] The documents contained a memo and a series of essays that detailed the ways in which video games, even those video games that do not directly connect to the Internet, could be used as recruitment and communication tools for terrorists.[3] However, these operations have brought about privacy concerns for some who worry that their government could or would listen to their conversations as they are playing these videos games.[4] It is not clear how the government collected or accessed the data or communication from these video games.[5] It is likely that government agents created their own profiles and avatars in these games to access the virtual worlds. Additionally, privacy concerns have not be assuaged by the fact that there is no indication from the documents that any of the intelligence operations led to the foiling of any terrorist plots or to the arrest of any criminal.[6] The National Security Administration ("NSA")

---

[1] *NSA files: games and virtual environments paper*, THE GUARDIAN (Dec. 9, 2013), http://www.theguardian.com/world/interactive/2013/dec/09/nsa-files-games-virtual-environments-paper-pdf; *See* James Ball, *Xbox Live among services targeted by US and UK spy agencies*, THE GUARDIAN (Dec. 9, 2013, 6:26 PM), http://www.theguardian.com/world/2013/dec/09/nsa-spies-online-games-world-warcraft-second-life.

[2] *See* Ball, *supra* note 1.

[3] *See NSA documents on games and virtual worlds,* PROPUBLICA, http://www.propublica.org/documents/item/889134-games (last visited on Feb. 14, 2014) [hereinafter *NSA Documents*].

[4] Ball, *supra* note 1.

[5] *Id.*

[6] *Id.*

and the federal government may have free reign to spy on foreign peoples and foreign governments, but under the U.S. Constitution it does not have the legal authority to spy on American citizens without a warrant.[7]

Online video games have players who live across the globe and within the United States. Many of the computer servers on which the video games operate and communicate are inside of the United States.[8] Since the intelligence collecting process has not been revealed, it is unclear if the NSA or other federal agencies have been accessing the data and the monitoring communications of innocent Americans whose identity and nationality may have been concealed behind their virtual avatar.[9] The debate over the expectation of privacy concerning different types of Internet communication is growing, especially concerning social media.[10] Violations of privacy could hinder player anonymity, which is a key component of certain types of online gaming that encourages escapism. On the other hand, ending anonymity could encourage fairer and more civil discourse in the virtual gaming worlds.[11] The revelations of these documents has led to the question of whether there are any expectations of privacy for video game players and the communications between players which occur within those video games.

---

[7] *See* U.S. CONST. amend. IV.

[8] For Example, *World of Warcraft*, which is owned and operated by Blizzard Entertainment, has over seven million subscribers around the world, servers that run the game processes around the world, and their headquarters are here in the United States. *See Privacy Policy*, BLIZZARD ENTM'T (last updated July 28, 2014), http://us.blizzard.com/en-us/company/about/privacy.html [hereinafter Blizzard's Privacy Policy]; *See also* Luke Karmali, *World of Warcraft down to 7.7 Million Subscribers*, IGN (July 26, 2013), http://www.ign.com/articles/2013/07/26/world-of-warcraft-down-to-77-million-subscribers.

[9] Ball, *supra* note 1.

[10] Bryce Clayton Newell, *Rethinking Reasonable Expectations of Privacy in Online Social Networks*, 17 RICH. J.L. & TECH. 12, 12-13 (2011).

[11] Jaikumar Vijayan, *Gaming giant Blizzard ends online anonymity, stirs up storm*, COMPUTERWORLD (July 9, 2010), http://www.computerworld.com/s/article/9179042/Gaming_giant_Blizzard_ends_online_anonymity_stirs_up_storm.

This note will review many different aspects of online video games and video game communications in the world after the leaks shown by Edward Snowden. This note will first examine whether or not there is a difference between video game consoles and computers that could affect the application of the law. Next, the note will discuss the many interests the government may have for monitoring the activity of online video game players, followed by a survey of privacy laws in the United States and how they could affect online video games. The note will then discuss anonymity in video games and if that element of anonymity is enough to warrant an expectation of privacy. Finally the note will discuss how the big businesses that make these online games handle private information and how that may affect a gamer's expectation of privacy.

I. COMPUTERS VERSUS VIDEO GAME CONSOLES

The definition of a computer is becoming blurred, but this does not have an effect on the legal expectations of the user. For legal purposes, the most important factor is ability of both computer and video game consoles to connect to the Internet. This connection to the Internet is important because this places the gaming system in connection with interstate commerce.

For those not familiar with the different between video game consoles and computers, there is very little difference between the hard ware and software used for video games played on either a computer or video game console. For computers, computer games are downloaded to the player's computer either from a disk or an Internet service platform, such as Steam.[12] Once the game is installed onto the computer and the computer is connected to the Internet, the player can

[12] *Welcome to Steam*, STEAM, http://store.steampowered.com/about/ (last visited Sept. 16, 2014); Bradley Mitchell, *Online Games: Using computer networks to play games online*, ABOUT.COM, http://compnetworking.about.com/od/homenetworkuses/a/network-online-games.htm (last visited Sept. 16, 2014).

then access game.[13] The Internet connection of course is provided by the user's router or Internet Service Provider, such as Comcast, Optimum, or Verizon. Once inside a game, the player is usually prompted to create an avatar or profile to access the online components of the game.[14] That avatar is how the player will be represented to the rest of the online game's community.[15]

Console gaming requires that the player first own such a console, such as the PlayStation 4 or Xbox One. Each game console manufacturer maintains its own separate Internet service for online games. This Internet service then connects to the player's local router, just like a computer. Xbox consoles connect to Xbox Live and PlayStation consoles connect to The PlayStation Network. In order to access the consoles features, the player must create a profile for the particular network that the console is connected.[16] This profile will be the avatar and profile that appear for all games that the player plays on that network. [17] For the newer consoles including Xbox One and PlayStation 4, the player must also pay a subscription fee in order to access the network. Once the player has set up their profile they may either install a video game through a disk or download it from the console's network. [18] Once installed the player can access the game's online features, which in turn connect to the Internet through the console's network. [19] Newer consoles, such as the PlayStation 4 and the Xbox One, also allow for the download of

---

[13] Mitchell, *supra* note 12.

[14] *World of Warcraft Beginner's Guide: Chapter 1 Getting Started*, BATTLE.NET, http://us.battle.net/wow/en/game/guide/getting-started (last visited Sept. 16, 2014) [hereinafter *World of Warcraft Beginner's Guide: Chapter 1*].

[15] *Id.*

[16] Kathryn Montminy, *How to Create a PlayStation Network Account,* ABOUT.COM, http://psp.about.com/od/pspforkids/ss/How-To-Create-A-Playstation-Network-Account.htm (last visited Sept. 16, 2014).

[17] *Id*.

[18] *Id.*

[19] *Id.*

applications that allow a user to connect to websites and other Internet based services, such as Amazon Prime and Netflix through their network.[20] These capabilities of newer consoles further blur the line between console and computer.

Additional complications arise when discussing mobile gaming devices and mobile phones. Mobile phones have the ability to access the Internet through both wireless communications provided by an Internet provider and through "3G" or "4GLTE" networks maintained by cellphone carriers such as AT&T and Verizon.[21] Additionally, hand held devices specifically made for playing video games, such as the PlayStation Vita, can connect to the console manufactures network. Specifically, the PlayStation Vita can also connect to Sony's PlayStation Network. [22] The mobile or handheld device can either connect to the Internet through "3G" provided by a cell phone company such as AT&T or by connecting an USB cable or Bluetooth connection to a correlated video game console. Thus, in the case of the PlayStation Vita it can connect to the Internet through the PlayStation 3 or PlayStation 4.[23]

The difference between console gaming and computer gaming does not lie in the hardware of the console or the computer and does not lie with their ability to connect to the Internet. The difference may be in the software that the console uses and the essential purpose of the system. This is important as this note may use the term (or similar terms) "online video games" to discuss both games played on a computer and games played on a video game console. The essential purpose of the system and the online video games themselves may lead gamers to

[20] *PlayStation 4 Overview*, http://us.playstation.com/ps4/index.htm (last visited Feb. 14, 2014).

[21] Brian Jung, *How Does the Internet Work on Cell Phones?*, CHRON.COM, http://smallbusiness.chron.com/Internet-work-cell-phones-55688.html (last visited Feb. 16, 2014).

[22] Chelsea Stark, *PlayStation Vita: Everything you Need to Know,* MASHABLE (Feb. 22, 2012, 8:47 PM), http://mashable.com/2012/02/22/playstation-vita-faq/.

[23] *Id.*

have an expectation of privacy as discussed later in the note. Differing from computers, video game consoles and computers are not simply connecting to the Internet through a browser, thereby making many features of video games a concern of government.

II. WHY WOULD A TERRORIST OR CRIMINAL BE INTERESTED IN VIDEO GAMES?

Online video games create a number of issues for the government. However, the question that should be held in mind while reviewing those concerns is, if an expectation of privacy is found to exist, whether these issues warrant a breach of privacy by the government.

One of the major reasons that criminals or terrorists would be interested in online gaming is the massive amount of money being spent on virtual currencies and in game purchases.[24] Most online games use some sort of virtual economy or virtual currency to allow players to make purchases, with real money, while playing the game.[25] For example *Eve Online* has a massive player base with over 400,000 players participating in the game's virtual market.[26] *Eve Online* is a game where players build spaceships and traverse a virtual galaxy.[27] In order to build those virtual ships players can buy and sell raw materials which, in turn creates the game's own fluctuating commodities markets. Players of *Eve Online* can even form trade coalitions and banks.[28] Virtual economies have gotten so complicated that some video game companies have hired economic analysts to help them create and regulate the economies.[29] Since purchasing in

[24] Erik Kain, *Massive 'EVE Online' Battle Could Cost $500,000 In Real Money*, FORBES (Jan. 29, 2014, 4:55 PM), http://www.forbes.com/sites/erikkain/2014/01/29/massive-eve-online-battle-could-cost-500000-in-real-money/.

[25] Brad Plumer, *The Economics of Video Games*, WASH. POST (Sept. 28, 2012), http://www.washingtonpost.com/blogs/wonkblog/wp/2012/09/28/the-economics-of-video-games/.

[26] *Id.*

[27] *Id.*

[28] *Id.*

[29] *Id.*

the virtual worlds requires real dollars, these virtual currencies and economies can have real world consequence.[30] The NSA documents estimated that there is approximately one to two billion dollars' worth of intangible goods in the online game *Second Life*.[31] The NSA documents went on to chart the exchange rate for virtual currencies to real dollars for a number of online games.[32] With the ability to hide behind their avatars, criminals and terrorists could use these currencies to raise money or transfer money in the form of virtual currency to fund terrorist activity.

In addition to the flow of in-game cash, the leaked NSA documents specifically mention a game created by terrorist group Lebanese Hezbollah called *Special Forces 2*.[33] The NSA documents state that the game is sold for ten dollars a copy and that money goes to "fund terrorist organizations."[34] The NSA documents claim that this game contains multiplayer features that allow for online text and voice chat of up to 60 players.[35] The NSA documents claim that games like Hezbollah's *Special Forces 2* can be used for the recruitment and training of terrorists by providing weapons training and realistic battle field simulations.[36] It is ironic that this game, as the NSA documents point out, is based off another online game *America's Army*, which was produced by the United States Army for recruitment and training of United States troops and is free to download.[37] This could indicate a double standard. *America's Army* is currently on its

[30] *NSA Documents*, *supra* note 3.

[31] *Id.*

[32] *Id.*

[33] *Id.*

[34] *Id.*

[35] *NSA Documents*, *supra* note 3.

[36] *Id.*

[37] *Id.*

third iteration *America's Army 3* and has substantially similar goals of Hezbollah's *Special Forces 2*.[38] *America's Army 3* describes itself as a "stunningly realistic" experience that provides "authentic military elements including training, technology, weapons, and audio than any other military game."[39] Additionally, the in game play allows for multiplayer communication.[40] The hypocrisy is furthered by the fact that *America's Army 3* is currently free to download and play.[41] Hypocrisy aside, there may be some merit to the concerns of the government.

The biggest concern of the NSA documents is the ability of online games to provide easy communications between multiple players.[42] The NSA document gives examples of the types of communications online games offer including email, voice over internet protocol, chat, proxies and web forms. [43] The NSA documents detail how a single *World of Warcraft* player can set up a "guild" or group to coordinate and communicate verbally and non-verbally either in a group chat or player to player. [44] The NSA documents detail the government's worries that terrorist groups could use these same means of communication, almost anonymously, to communicate to each other. The NSA documents additionally consider the convergence of mediums that online games allow. [45] The NSA documents detail how soon, the MMO game *Second Life* may allow the game's players to text and voice call phone numbers almost anonymously. [46] The merger of

[38] *AA3 Home*, AMERICA'S ARMY 3, http://aa3.americasarmy.com/ (last visited Mar. 16, 2014).

[39] *America's Army 3*, STEAM, http://store.steampowered.com/app/13140/ (last visited Mar. 16, 2014).

[40] *Id.*

[41] *Id.*

[42] *NSA Documents*, *supra* note 3.

[43] *Id.*

[44] *Id.* at 33.

[45] *Id.* at 3.

[46] *Id.*

cellphones and online video games opens up the door to additional possibilities of communication. The NSA documents claim that all of these different types of communication offer terrorists essentially private meeting places that can be used for planning, collaboration, communications, and training. [47]

These concerns over communication in online video games are compounded by the fact that the NSA, with few exceptions, cannot differentiate the traffic of these online games from normal traffic on the Internet. [48] Therefore, in order to locate terror cells or criminals within the virtual world, the NSA would have to rely on human intelligence gathering practices, also known as HUMINT.[49] Absent new developments in searching capabilities by the NSA, this will be the method for the intelligence gathering for the foreseeable future. HUMINT could include government agents creating avatars and profiles in these online games. The government agents would access the game in order to recruit and mine for intelligence and data within the virtual world. [50] In fact, there were so many agents from different agencies within these gaming virtual worlds according to the NSA document that "de-confliction" groups were required to make sure the agencies intelligence operations were not interfering with each other.[51]

There are a series of questions that open up the NSA's operation to suspicion. Should the NSA, FBI, or any government entity or official play video games with the general public? Additionally, when the NSA is collecting in-game data, or intelligence on a certain player ID,

---

[47] *NSA Documents*, *supra* note 3.

[48] *Id.*

[49] *Id; News & Information*, INTelligence*: Human Intelligence*, CENTRAL INTELLIGENCE AGENCY (Apr. 30, 2013, 12:41 PM), https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/intelligence-human-intelligence.html

[50] *NSA Documents*, *supra* note 3.

[51] *Id.*; Ball, *supra* note 1.

avatar, or group, or guild of players, how does the NSA identify who the player is? What information about the player is collected? Is the NSA able to differentiate between American players and foreign players? If the NSA is able to match a player avatar to a certain console or computer through IP or MAC addresses, does that matching create a violation of privacy? Is there an expectation by the players to privacy or to maintain their avatars anonymously?

Many of the questions above cannot be answered because of the lack of specific operational details in the NSA documents and the lack of governmental transparency. Additionally, there are many other popular types of communication which may be in the government's interest to monitor. But, if the government's fears are realized then the government may have an argument for monitoring online video game communication.

A. Are the Government's Fears Legitimate?

The government's fears may be legitimate. Although the NSA documents do not claim to show any success in preventing terrorism, there are news stories that could show some support to the government's fears.

In 2010, a teenager in Victoria, British Columbia was sentenced to life in prison after confessing to rape and murder over the chat logs of *World of Warcraft*.[52] The chat logs were only one part of a mountain of evidence used to convict him.[53] The teenager said he had bragged about his crime while playing *World of Warcraft* because he thought the chat logs were less likely to be saved.[54]

---

[52] Justin Olivetti, *Teenager Killer Confesses Crime in World Of Warcraft Chat, Sentenced to Life in Prison*, ENGAGET (Nov. 5, 2011, 12:00 PM), http://massively.joystiq.com/2011/11/05/teenage-killer-confesses-crime-in-world-of-warcraft-chat-senten/.

[53] *Id.*

[54] *Id.*

Another incident occurred in 2011, when FBI agents arrested two students for allegedly fraudulent sales and purchases of virtual currency while playing *World of Warcraft*.[55] According to a government document made public by the whistleblower and hacker group LulzSec, criminal syndicates and gangs such as MS-13 used PlayStation 3 and Microsoft Xbox 360's live chat features to communicate with each other in order to recruit members and conduct criminal activity.[56] These documents were released in 2010 and detailed how the gang specifically used video game communications to communicate covertly to group members overseas in order avoid detection by police. [57]

It is, of course, arguable that these are isolated incidents. Since the NSA documents do not show any concrete evidence of successful terrorism prevention, it is difficult to balance or measure the true threat level that these types of communications possess. Thus, if there is an expectation of privacy, it may be hard to balance a possible danger (or lack thereof) against the violations of that privacy. However, if there is no expectation of privacy than the balancing of privacy versus police power may not be necessary.

III. VIDEO GAMES AND PRIVACY

There have been numerous attempts to regulate video game content, especially violence in video games. The documents leaked by Edward Snowden brought privacy concerns to the forefront of American political debate. Many of the surveillance programs began in the early

[55] Darlene Storm, *Intelligence Agencies Hunting for Terrorists in World of Warcraft,* COMPUTER WORLD (Apr. 13, 2011, 7:41 PM), http://www.computerworld.com/article/2471127/endpoint-security/intelligence-agencies-hunting-for-terrorists-in-world-of-warcraft.html.

[56] *(U//LES) LulzSec Release: New Jersey Fusion Center: MS-13 Using Game Consoles to Communicate*, PUBLIC INTELLIGENCE (June 25, 2011), https://publicintelligence.net/ules-lulzsec-release-new-jersey-fusion-center-ms-13-using-game-consoles-to-communicate/.

[57] *Id.*

2000s in response to September 11th terrorist attacks with the intention to prevent other terrorist threats. But there are no specific laws that focus on communication within video games. Thus, the focus remains on the protection of privacy in general, privacy on computers and general Internet communication.

A. Privacy Law

Griswold v. Connecticut first established a United States citizen's right to privacy, stating that the Bill of Rights has "penumbras, formed by emanations from those guarantees that help give them life and substance."[58] Stated without the weird term "penumbra," the Supreme Court found that a right to privacy must exist because the idea of a right of privacy is interwoven in the principles and ideas of the Bill of Rights.[59] *Griswold v. Connecticut* dealt with the prohibition of the use of contraceptives.[60] Although the case is far too old to deal with technological issues, it does set a precedent of expectations of privacy within one's own home.

One of the most famous examples of technology versus privacy concerns that made its way to the Supreme Court occurred in *Kyllo v. United States*.[61] The police in *Kyllo* used a thermal imaging device, without a search warrant, to determine if the amount of heat emanating from the defendants home was consistent with the high-intensity lamps typically used for indoor marijuana growth.[62] As Danielle Keats Citron analyzed in her article, the Court was invited to limit Fourth Amendment protection to activities in the home that can be regarded as "intimate"

[58] Griswold v. Conn., 381 U.S. 479, 484 (1965).

[59] *Id.*

[60] *Id.* at 480.

[61] Kyllo v. United States, 533 U.S. 27 (2001).

[62] *Id.*

but chose not to do so.[63] The Court instead chose to focus on whether or not the activity was invasive. [64]

Another Supreme Court case, *United States v. Jones,* addressed the use of GPS tracking to monitor a specific persons movements and their connection to local drug activity in the District of Columbia.[65] In *Jones,* the defendant argued that the collection of data about his movement could lead to the incidental collection of intimate details of his life and therefore a violation of his privacy.[66] Here, the court again dodged the issue of intimate privacy in one's own home.[67] The Court in *Jones* held instead, that the defendant's rights were violated not because of an expectation of privacy, but instead because law enforcement physically occupied his private property for the purpose of obtaining information on the defendant.[68] David Witte contends that in their ruling in *Jones*, the Supreme Court sought to avoid ruling that there was a reasonable expectation of privacy in an individual's location on Earth.[69] He contends that instead, the Supreme Court established a constitutional minimum. [70]

---

[63] Danielle Keats Citron & David Gray, *Addressing the Harm of Total Surveillance: A Reply to Professor Neil Richards*, 126 HARV. L. REV. 262, 268 (2013).

[64] *Id*. at 268.

[65] United States v. Jones, 132 S. Ct. 945, 949 (2012).

[66] *Id.* at 948.

[67] Derek S. Witte, *Privacy Deleted: Is It Too Late to Protect Our Privacy Online?,* 17 J. Internet L. 1, 16 (2014) [hereinafter Witte, *Privacy Deleted*] (citing United States v. Jones, 625 F.3d 766 (D.C. Cir. 2010)).

[68] *Id.* at 16.

[69] Derek S. Witte, *Bleeding Data in a Pool of Sharks: The Anathema of Privacy in a World of Digital Sharing and Electronic Discovery*, 64 S.C. L. REV. 717, 738 (2013) [hereinafter Witte, *Bleeding Data*].

[70] *Id.*

B. Legislative Protections of Privacy

Prior to the Snowden leaks, not much had been written regarding privacy concerns and video games. Additionally, there has not yet been a Supreme Court case determining the legality of the NSA's video game or Internet surveillance programs. Therefore, it may be prudent to look for congressional action or legislation for indications on whether there are any privacy protections for video games.

In the article *Bleeding Data in a Pool of Sharks: The Anathema of Privacy in a World of Digital Sharing and Electronic Discovery* in the *South Carolina Law Review*, Derek Witte provides a comprehensive chart concerning various federal statutes concerning personal data shared online.[71] Witte analyzes that there may be little protection for personal data on social networking sites through federal statutes. [72] But the question remains if the same can be said about online gaming.

The two relevant statues on Witte's chart are the Wire Tap Act and the Electronic Communications Privacy Act. The Wiretap Act made it unlawful for any individual to intercept a communication to which they are not a party. [73] There is an exception for law enforcement, but they may do so only with a valid court order. [74] In 1986, the Electronic Communications Privacy Act extended the protections to include electronic communications. The act defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo-electronic

---

[71] *Id.* at 742-748.

[72] *Id.*

[73] Witte, *Privacy Deleted*, *supra* note 67, at 1-16.

[74] *Id.*

or photo-optical system that affects interstate or foreign commerce."[75] The Stored Communications Act added stored communications to the list of protected types of electronic communications.[76] The Electronic Communications Privacy Act has since been affected or amended by the USA Patriot Act and the Foreign Intelligence Surveillance Act.

The Foreign Intelligence Surveillance Act ("FISA") gives procedures to the government to conduct physical and electronic surveillance of "foreign intelligence information" between "foreign powers" and "agents of foreign powers."[77] The part of the statue to note here is the fact that "agents of foreign powers" includes possible United States citizens. Thus, the statue attempts to protect United States citizens by requiring that in order for the government to conduct the surveillance, the government must obtain a warrant and show probable cause.[78] Alone this may seem as sufficient protection, however it has come to light that while conducting surveillance on foreign targets, the government has "incidentally" obtained data on United States citizens.[79] These fears of over the extension or additional "incidental" collection of data is compounded when taking into account the amount of personal and private data that can be gleaned from private computers and video game consoles.

IV. IS THERE AN EXPECTATION OF PRIVACY IN THE VIRTUAL WORLD?

According to the NSA documents as discussed above, the NSA has very limited capabilities when trying to identify and pierce the Internet traffic of online games. Accordingly,

[75] 18 U.S.C. § 2510 (2002).

[76] 18 U.S.C § 2701 (2014).

[77] 50 U.S.C. § 1801 (2010).

[78] Act of Oct. 25, 1978, Pub. L. 95-511, 92 Stat. 1783.

[79] Chris Strohm, *NSA Phone Data on U.S. Locations Incidental Chief Says,* BLOOMBERG BUSINESS (Dec. 11, 2013, 4:35 PM), http://www.bloomberg.com/news/2013-12-11/nsa-phone-data-on-u-s-locations-incidental-chief-says.html.

the NSA documents revealed that strategies in collecting intelligence within online games involve HUMINT as well as the creation of profiles and avatars by government officials.[80] This tactic appears may have important legal difference from the collection of big data. Much like social media, a large portion of online games occurs in a virtual world that is open to everyone that has a profile or avatar in that game.[81] But does this mean that the government then has the right to create its own avatar and participate in the online world? Courts have not reached a conclusion as to whether the fourth amendment reaches spaces on the Internet.[82]

Since there are many different types of communication and activities in video games, it might be reasonable to expect different levels of protection within the online game. For example, in the game *Second Life*, the player can create many different types of structures and virtual places for their avatar to "live" or with which to interact.[83] These creations could present many possible scenarios that could indicate a level of expectation of privacy. It also raises the question of how the virtual home should be treated. On one hand, if another player were to try and access the virtual home, the player would have the ability to choose whether or not the other player can enter. [84] This could give a player a sense of privacy and autonomy.[85] On the other hand the online game and the virtual home is simply virtual code that passes along through the Internet and into the public commerce. Additionally, does the expectation of the player change since the company that runs the online game will always have access to the code that creates the virtual world it

[80] *NSA Documents*, *supra* note 3.

[81] *World of Warcraft Beginner's Guide: Chapter 1*, *supra* note 14.

[82] Marc Jonathan Blitz, *Stanley in Cyberspace: Why the Privacy Protection of the First Amendment Should Be More Like That of the Fourth*, 62 Hastings L.J. 357, 372 (2010) [hereinafter Blitz, *Stanley in Cyberspace*].

[83] *Create*, SECOND LIFE, http://secondlife.com/whatis/create/?lang=en-US, (last visited Feb. 16, 2014).

[84] *Id.*

[85] Blitz, *Stanley in Cyberspace*, *supra* note 82, at 375-376.

maintains? Marc Blitz argues that there may be a sense of trust and an expectation of privacy between players and the companies that create the game.[86] This trust, he argues, is similar to bank and phone records that require the government to obtain a warrant before the company divulges any information. [87] Blitz notes that the Supreme Court has been hesitant to extend protections of privacy where the information is open to the public.[88] Thus the question of an expectation of privacy may still be up for debate.

If the government agent only maintains access to the public areas of the online world, then the agent most likely can avoid privacy breaches and act similar to a mole or undercover officer. As discussed, there may be little in the eyes of the law that a player should expect in terms of privacy in public spaces.[89] And while the government may be able to view the public information on a gamer's avatar or profile, it needs assistance in some form to identify the people behind the avatar. This leads to either two situations: either the government asks or subpoenas the gaming company, or the government uses data mining programs or hacks a player's account. Either situation could tread on a fundamental piece of some online video games or that is anonymity.

A. Anonymity

At first glance, video games and communication through video games looks a lot like social media, such as Facebook or Twitter, and usual Internet communication, such as Skype or any other type of video chat. But one of the most important factors of certain types of video

[86] Blitz, *Stanley in* Cyberspace, *supra* note 82, at 376.

[87] *Id.*

[88] *Id.*

[89] *Id.*

games is the ability to "virtually" become a different person, and he idea that video games are a form of escapism is not new.[90]

The ability to hide behind a user name in place of a real name is an enticing one for criminals. But, it can also allow for a video game player to be expressive and communicate in ways that the player does not feel is possible in the real world.[91] This expression can be both negative and positive. John Suler proposes that this phenomenon, known as "The Online Disinhibition Effect," is responsible for the callous behavior often seen in YouTube video comments.[92]

The Online Disinhibition Effect is made up of various components: Dissociative Anonymity, Invisibility, Dissociative Imagination, and Minimization of Authority.[93] Together these factors give an Internet user or online gamer the ability to act without, or to feel as if they are acting without, taking responsibility for their own actions.[94] The Online Disinhibition Effect applies not only to comments on YouTube, but also to online gaming. This decreases the Internet user or gamers inhibitions and gives them the freedom to act outside of their comfort zone.[95] While it allows the players certain freedoms and privacy, it can also have negative effects.

---

[90] Gordon Calleja, *Digital Games and Escapism*, ACADEMIA.EDU, http://www.academia.edu/2962309/Digital_Games_and_Escapism (last visited Sept. 19, 2014).

[91] *See* Marc Jonathan Blitz, *A First Amendment for Second Life: What Virtual Worlds Mean for the Law of Video Games*, 11 VAND. J. ENT. & TECH. L. 779 (2009).

[92] *See* John Suler, *The Online Disinhibition Effect*, 7 CYBERPSYCHOLOGY & BEHAVIOR 321 (2004), *available at* http://online.liebertpub.com/doi/pdf/10.1089/1094931041291295.

[93] Cam Robinson, *Reality Check - Why Are Online Gamers Jerks? (Video),* GAMESPOT (Nov. 10, 2013), http://www.gamespot.com/videos/reality-check-why-are-online-gamers-jerks/2300-6416026/ (last visited Feb. 15, 2014) (citing Suler, *supra* note 92).

[94] *Id.*

[95] *Id.*

A recent study conducted by the Nanyang Technological University and Singapore and Shanghai Jiao Tong University found that anonymity, among other things, does, in fact, make individuals more likely to cheat and engage in bad behavior.[96] However, the researchers also found that the players considered themselves to be part of a social group where the norm was to cheat, which may have attributed to the cheating. [97] Thus, the study claimed that socials norms, such as cheating, could be subject to change. [98] Additionally, the study concluded that cheating may not be part of anonymous gaming, but instead anonymous gaming could create social groups and a sense of belonging. [99]

While the arguments over mean YouTube comments or angry "Tweets" from peoples' Twitter accounts rage on, it is important to note that there is a difference between common Internet communications and online video game worlds. Many of these virtual worlds were specifically created to give players the ability to "escape," become someone else, or assume the roles of heroic fantasy characters.[100] For many people this is a chance to create their own private story.[101] In the case of *Second Life*, a large portion of the game's environment, and the core element of the game, is based around the idea of a living out a life separate from the player's real life, generating your own stories and experiences.[102]

---

[96] Chris Pereira, *Anonymity Encourages Bad Behavior in Online Games,* IGN (Jan. 9, 2014), http://www.ign.com/articles/2014/01/09/anonymity-encourages-bad-behavior-in-online-games.

[97] *Id.*

[98] *Id.*

[99] *Id.*

[100] *What is World of Warcraft*, WORLD OF WARCRAFT, http://us.battle.net/wow/en/game/guide/ (last visited Sept. 14, 2014).

[101] *Id.*

[102] *What is Second Life?*, SECOND LIFE, http://secondlife.com/whatis/?lang=en-US (last visited Sept. 14, 2014).

Thus, the aspect of anonymity could indicate an expectation of privacy for many gamers. There may be an expectation from the gamer when they create an avatar in an online video game that they have some privacy. This is compounded by the fact that most gamers play within their own homes and on their own video game consoles. As discussed above, until recently many video game consoles sole purpose was to play these video games. But the release of the new consoles and the development of inter woven cellphone apps and social media has affected gaming in many ways, which could hinder online video game player's expectation of privacy.

B. Non-legal Remedies To Government Fears of Anonymity?

Video games used to be separated from social media, however that difference has recently started to erode. Many video game companies and social media companies have started to provide ways to link player's social media accounts to their online video game accounts.

In 2010, *World of Warcraft* and *Second Life* changed their privacy policies for the forum comments.[103] The online games now require that certain forum postings by a player must use their real names. Blizzard Entertainment Inc., which runs *World of Warcraft*, has since implemented a new system called Real ID.[104] Real ID is a system that allows a player to link their in-game avatar with their account information, including their full names. [105] While Blizzard does place restrictions on which of the gamers fellow players can see the Real ID information, it does allow Blizzard to view that information.[106]

---

[103] Vijayan, *supra* note 11.

[104] *Id.*

[105] *Id.*

[106] Blizzard *Privacy Policy*, *supra* note 8.

In 2013 Google sought to address vicious comments on YouTube by requiring that YouTube accounts be linked to Google+ accounts.[107] Google+ is the Google equivalent of Facebook, and requires that a member's photo and name be associated with their account.[108] Thus, if there is a chance that a post can be associated to an actual person, then there is less of a chance that the comment will be mean or cruel. [109]

Many video game companies have followed suite, including the PlayStation Network and Xbox Live. PlayStation Network now allows and encourages users to connect their PlayStation Network accounts to their social medial accounts.[110] Sony has also included new features in their Play Station 4 that give players additional abilities to share their in-game activities with other players. Sony went as far as to include a share button on their new gaming controllers for the PlayStation 4.[111] These new sharing tools allow the gaming companies to collect more data on their users and better identify either trouble or dangerous users. But these features also end a large amount of anonymity once enjoyed by the gamers. While the features and privacy features are controllable, it definitely removes some of the expectations of privacy from video games.

Cam Robinson, a journalist at GameSpot, proposes that a possible way to address online gaming anonymity is through the Kinect.[112] If the player's face or eyes could be associated or even seen by other players, then video game users might be more inclined to be less callous

---

[107] Paul Tassi, *Google Plus Creates Uproar Over Forced YouTube Integration,* FORBES (Nov. 9, 2013, 10:24AM http://www.forbes.com/sites/insertcoin/2013/11/09/google-plus-creates-uproar-over-forced-youtube-integration/.

[108] *Id.*

[109] *Id.*

[110] Stephen Totilo, *Study The PS4's Social Network Settings Before Putting It Online*, KOTAKU (Nov. 13, 2013, 4:30 PM), http://kotaku.com/these-are-the-social-network-settings-your-ps4-would-li-1463946510.

[111] *Social Sharing and Connectivity*, IGN, http://www.ign.com/wikis/playstation-4/Social_Sharing_and_Connectivity (last visited Feb. 16, 2014).

[112] Robinson, *supra* note 93.

towards each other.[113] Reducing anonymity online and in video games could lead to a reduction in the attitude of the players towards each other and reduce the possibility criminals seeing video games or Internet communications as viable options to avoid the police. Thus, associating a person with their own online persona could have implications in the legal world. Ending anonymity in gaming could end a criminal's use of video games as a vehicle to commit crimes.

It could be argued that due to the nature of gaming and gamers there is no need for ending anonymity. Gamers tend to be self-regulating. Most large gaming companies hire "moderators" to monitor the activity of the players for cheating and rude behavior that could otherwise ruin the game for the other players. For example, *World of Warcraft* employs "Game Masters" who can chat in game with players to monitor and report on in game activity that violates their terms of use policies for the game.[114] Additionally, many games include a reporting system where players can report the abuse and cheating of other players. For example, online video games that are installed and operated on a computer through Steam use the "Valve Anti-Cheat System" which includes the ability for gamers to report other gamers who cheat.[115] An extreme example of gamer self-regulation occurred when a teenager in Austin, Texas was flagged and reported to the police for a comment the player had made while playing *League of Legends* - an online multiplayer game - about shooting a school full of kids.[116] The teenager allegedly made the comment jokingly, but a woman in Canada was able to look up the teenager's

[113] *Id.*

[114] *Game Master Interaction, Battle.net Support*, BLIZZARD ENTM'T. (last updated Oct. 18, 2014), https://us.battle.net/support/en/article/game-master-interaction-policy.

[115] *Valve Anti-Cheat System (VAC)*, *Steam Support*, VALVE CORP., https://support.steampowered.com/kb_article.php?ref=7849-Radz-6869 (last visited Mar. 10, 2015).

[116] Robby Soave, *Texas teen makes violent joke during video game, is jailed for months*, DAILY CALLER (June 27, 2013, 8:02 PM), http://dailycaller.com/2013/06/27/texas-teen-makes-violent-joke-during-video-game-is-jailed-for-months/.

address and report him to the Austin Police. The police charged him for making a terrorist threat.[117] These new additions to the online video game industry make it increasingly hard for gamers to argue for an expectation of privacy.

If companies included illegal or suspicious behavior to the list of reportable offenses, government agencies such as the NSA and the FBI would not need to have their own players in the game. However, as stated in the NSA documents, it is difficult for the NSA to differentiate between online gaming traffic and regular Internet traffic.[118] This has led to government agents creating their own avatars and profiles in games in order to search for terrorists and criminals. [119] But, that method is, of course, limited if the government cannot access or identify the people behind the avatars. Thus, the government must rely on the big businesses to provide them with the data and intelligence.

V. VIDEO GAMES AND BIG BUSINESS

Derek Witte makes the argument that the United States Supreme Court has openly opposed the creation of "Big Brother" but that "Big Brother" already exists in the form of major tech companies such as Google and Facebook.[120] He goes on to argue that lawmakers must step up to protect the fundamental right of privacy before it is lost.[121] Witte contends that lawmakers must fight for new legislation because consumers, the average citizen, are powerless to bring about such changes to protect privacy.[122] With the massive amounts of data that could be

[117] *Id*.

[118] *NSA Documents*, *supra* note 3.

[119] *Id.*

[120] Witte, *Privacy Deleted*, *supra* note 67, at 13.

[121] *Id.*

[122] *Id.*

collected through video game avatars, profiles, and video game purchases, these concerns extend to the online gaming world. Or is there something different about video games and video game consumers?

At the time it was announced, the new Xbox One was met with a surprising controversy concerning one of its technologies, the Kinect. The new Xbox One comes with Kinect, a technology that combines a camera and microphone, which allows the consumer to interact with the Xbox One through hand motions and voice commands.[123] The Kinect has incredible capabilities that allow it to recognize individuals.[124] At their announcement of the Xbox One, Microsoft stated that their new console would be always connected to the online servers. After the announcement, consumers became concerned that the Xbox One would always be on, and through the Kinect, the Xbox One would be watching their every move, even when they were not playing video games.[125] Microsoft insisted that the Kinect was an essential and integrated part of the Xbox One and thus need to be plugged in all the time to the Xbox One.[126] Player's fears were compounded when they learned soon after the Xbox One announcement that Microsoft had provided the NSA and the FBI with encryption workarounds needed to access other Microsoft products, such as Skype video calls, Outlook email, and online chats.[127] While Microsoft has not given a clear reason regarding the reverse in policy, months later Microsoft quietly removed the

---

[123] *Xbox Privacy Statement*, MICROSOFT (last updated Nov. 2014), http://www.microsoft.com/privacystatement/en-us/xbox/default.aspx.

[124] Brian Crecente, *Privacy concerns threaten to overshadow Microsoft's new console*, POLYGON (June 5, 2013, 11:14 AM), http://www.polygon.com/2013/6/5/4398440/privacy-microsoft-xbox-one.

[125] Yannick Lejacq, *Game on for surveillance? Privacy advocates concerned over new consoles,* NBC NEWS, http://www.nbcnews.com/tech/video-games/game-surveillance-privacy-advocates-concerned-over-new-consoles-f6C10732136 (last visited Feb. 16, 2014).

[126] *Id.*

[127] Larry Frum, *Microsoft backtracks on Xbox One sharing policies*, CNN (last updated June 21, 2013, 12:45 PM) http://www.cnn.com/2013/06/19/tech/gaming-gadgets/xbox-drm/.

always-on feature for the Xbox One and changed their Privacy Policy.[128] Thus, consumers and media attention was able to create a change in a company's privacy policy.

But has that event made a serious impact on what data Microsoft, Sony, and other online gaming companies collect? The answer is: not really. Microsoft still collects data from the Kinect and so do most online video game companies.[129]

A. Have Gamers Given Up Their Privacy Rights?

New data analytics have opened new doors for gaming companies.[130] In the gaming context, analytics use in-game data and information gathered from the player's actions as a way of learning gamers' behavioral patterns while the play. [131] This allows the companies to learn many things about their players, such as when and for how long gamers view a specific advertisement. [132] Additionally, for a fee, the companies are able to forward the data to online players, thereby allowing the players to use the data to improve their own gaming skills. These data collection improvements often come at a price. The video game company could use analytics to collect private data about a player's Internet usage among other private information. [133] Often, many companies do not update their privacy policies to inform the players about the

---

[128] *Id.*

[129] *Id.*

[130] Joseph Gregory, *Analytics in Video Games: Gamer's Best Friend or Privacy Nightmare?*, N. Y. LAW SCHOOL INSTITUTE FOR INFORMATION LAW AND POLICY LEGAL BLOG NETWORK, *available at* http://web.archive.org/web/20130601192517/http://www.allyourlawarebelongtous.com/analytics-in-video-games-gamer%E2%80%99s-best-friend-or-privacy-nightmare.

[131] *Id.*

[132] *Id.*

[133] *Id.*

collection of this data, and in order to gain access to MMO's the player has often already given authorization to the company to collect the data. [134]

What types of personal and private information do these video game companies actually have access to? Blizzard Entertainment's privacy policy may be a good analysis of a company's information policies. Blizzard owns and created some of the most popular massive multiplayer online games to date, including *World of Warcraft*, *StarCraft* and *Diablo*.[135] As Blizzard Entertainment's privacy policy states, the company may collect information concerning the consumer's:

> (1) the purchase of goods or services though our on-line stores, (2) product or account registration, or registration for on-line game participation, (3) player match-up services, (4) message boards or forums, (5) eCards or Recruit-a-Friend e-mails, (6) warranty registrations, (7) contest registrations, (8) a consumer complaint, (9) surveys, (10) customer service or technical support, and/or (11) newsletters. Personal information collected may include your name, home address, phone number, and/or e-mail address.[136]

Blizzard is quick to point out that the information is always given up voluntarily. Of course that does not mean that you will have access to the online game if you refuse to give up the information. "We do not require this information to gain access to our sites, however, you will not be able to utilize certain products, services, or features that require registration or receive materials such as newsletters unless such information is provided."[137] Like many video game companies, Blizzard uses the consumer's personal information to create analytic data "for

---

[134] *Id.*

[135] Blizzard's Privacy Policy, *supra* note 8.

[136] *Id.*

[137] *Id.*

internal marketing, profiling, or demographic purposes."[138] As discussed above this could have both positive and negative consequences.

More interesting information on Blizzard Entertainment's Privacy Policy is contained within the section describing with whom Blizzard may share this information with. This includes third party vendors who fulfill product orders or prizes, process mailings, or process, analyze, and/or store data on Blizzard's behalf.[139] In addition to third party vendors, Blizzard also claims your information as an asset of their company, "as with any business, your personal information is also an asset of Blizzard and will become part of our normal business records. As such, we may also disclose your personal information to a third party if we decide to sell a line of business to that third party…"[140] The the privacy policy does not clearly identify these third parties. At a minimum, Blizzard is partnered with at least twenty-one companies that create ancillary products, such as board games and manga, for their game universes.[141] Accordingly, at least twenty-one companies may have access to the consumer's information than the consumer may have intended.

Additionally, Blizzard keeps track of Internet Protocol ("IP") addresses, which is the unique number assigned to an individual user's server or Internet Service Provider ("ISP").[142] IP's allow site tracking and can be used for security purposes.[143] But the information can also be

[138] *Id*.

[139] *Id.*

[140] Blizzard's Privacy Policy, *supra* note 8.

[141] Manga are Japanese comics and graphic novels. *Partners*, BLIZZARD ENTM'T, http://us.blizzard.com/en-us/company/about/partners.html (last visited Feb. 16, 2014).

[142] Blizzard's Privacy Policy, *supra* note 8.

[143] *Id.*

used to report aggregated information. [144] Tracking and server information can be used to determine the location of a computer or console.[145]

Furthermore, when all of the data collected by the company is viewed together, the gaming companies can create vastly detailed pictures of the activity that occurs on a player's computer or gaming console.[146] Some consumers do not even realize they are forfeiting their personal information to major corporations. [147] Most consumers have not considered what might happen after they hand over their data. [148] While the government is limited by legislation on the sale and use of our personal information, private companies are not limited. [149] Corporations bear the burden of maintaining the cloud storage and the physical servers that process and store all of their online games' processes and information, which is not cheap. [150] However, the usage and buying or selling of our personal information to marketing companies or corporate partners can be lucrative.[151]

There is also the issue as to whether or not these companies comply or assist the government in pursuing criminals and terrorists. The Privacy Policy states that Blizzard will comply with any disclosure requirements mandated by law, or if the players' actions or conduct may cause harm to any other party either intentionally or unintentionally, and to anyone else who

---

[144] *Id*.

[145] Stephanie Crawford, *What is an IP address?*, HOWSTUFFWORKS, http://computer.howstuffworks.com/Internet/basics/question549.htm (last visited Feb. 16, 2014).

[146] Witte, *Bleeding Data*, *supra* note 69.

[147] *Id.*

[148] *Id.*

[149] *Id.*

[150] *Id.*

[151] Jason Morris & Edward Lavandera, *Why Big Companies buy, sell your data,* CNN (last updated Aug. 23, 2012, 3:52 PM), http://www.cnn.com/2012/08/23/tech/web/big-data-acxiom/.

could be harmed by the activities.[152] Because the government limits the amount of disclosure, it is unclear how much personal information companies divulge to the government.[153]

Previously, the government had a gag order on companies preventing them from even disclosing the fact that requests for data were made by the government. [154] It was only after the document leaks by Edward Snowden that the government slightly relaxed this policy. [155] Of course the transparency reports later released by the companies may be unreliable as companies only release information they feel necessary to reassure customers. [156] It would be more effective if the government were more transparent and released the information on the data requests themselves. [157]

To Blizzard's credit, it does provide clear statements regarding when and how players can opt out of programs. [158] Additionally, Blizzard claims to have taken steps to assure that all the information they collect will remain secure, such as partnering with Truste, a data protection company. [159] However, Blizzard refuses to guarantee the security of the information that is in the hands of third parties. [160] With all the data and access a gamer gives to a big video game company, it is not likely that a gamer would have any expectation of privacy from that company.

---

[152] Blizzard's Privacy Policy, *supra* note 8.

[153] Criag Timberg & Adam Goldman*, U.S. to allow companies to disclose more details on government requests for data*, WASH. POST (Jan. 27, 2014), http://www.washingtonpost.com/business/technology/us-to-allow-companies-to-disclose-more-details-on-government-requests-for-data/2014/01/27/3cc96226-8796-11e3-a5bd-844629433ba3_story.html.

[154] *Id.*

[155] *Id.*

[156] *Id.*

[157] *Id.*

[158] Blizzard's Privacy Policy, *supra* note 8.

[159] *Id.*

[160] *Id.*

The only remaining question is whether these companies will continue to support the government's actions.

B. Future Government and Businesses Action Together.

Companies will most likely continue to work with governments and governmental agencies. In exchange for user information from the gaming companies, government can provide both security and protection from criminals and civil remedies. These companies also seek to protect their own users from criminals and terrorists. Doing so is in their best interest, as breaches of data and fraud can hurt both their profits and public image. Government surveillance and technology can help companies avoid data breaches such as the PlayStation Network data breach in 2009.[161] The breach of Sony PlayStation Network in 2011 leaked a possible 77 million users' account information, including names, addresses, and possible credit card data, in one of the largest internet security break-ins ever.[162] The breach cost Sony an estimated 170 million dollars.[163] The company also faced lawsuits from private citizens and governments in the United States and Europe. [164] Thus, companies have an incentive to comply with government regulations that protect consumer data and government authorities that can help investigate if a breach occurs.

Businesses and governments are also acting together on many different issues. For example, in 2012, New York Attorney General Eric Schneiderman announced "Operation Game

---

[161] Liana Baker & Jim Finkle, *Sony PlayStation suffers massive data breach*, REUTERS (Apr. 26, 2011, 7:36 PM), http://www.reuters.com/article/2011/04/26/us-sony-stoldendata-idUSTRE73P6WB20110426.

[162] *Id.*

[163] IDT911, *Two Years On, Lessons Learned From the Playstation Data Breach,* IDENTITY THEFT 911 BLOG (MAY 13, 2013), http://www.idt911blog.com/2013/05/two-years-on-lessons-learned-from-the-playstation-data-breach/.

[164] *Id*.

Over."[165] The goal of the program was to remove all registered sex offenders from several online gaming services.[166] Over 3,500 accounts were removed by Microsoft, Apple, Blizzard, Electronic Arts, Disney, Warner Bros. and Sony, with each company consenting to the operation.[167]

Video game companies and big businesses are not in the business of data protection. They are in the business of making money for their shareholders. And while gamers may want to have a feeling of anonymity or privacy, that protection most likely does not exist.

CONCLUSION

Future technologies create increasing challenges to law enforcement officials and lawyers trying to keep up with the law. Richard Kemp states that prediction is the next big step on the road to the "Internet of everything," with "processors in your fridge to let you know when the yoghurt's going off or you're nearly out of milk; autonomous vehicles; expert systems; virtual helpers and other smart machines."[168] He predicts the growing consumer demand for social media and mobile data and an increase in cloud computer storage. [169]

The availability of alternate means of communication, such as pay as you go cell phones, and video chat programs, such as Skype, Facebook, and Internet chat rooms give criminals a wide range of communication options. The vast amount of different modes of communication,

---

[165] Richard Mitchell, *New York State removes sex offenders from Xbox live*, ENGADGET (April 5, 2012, 4:40 PM) http://www.engadget.com/2012/04/05/new-york-state-removes-sex-offenders-from-xbox-live-more/ (last visited Feb. 15, 2014).

[166] *Id.*

[167] *Id.*

[168] Richard Kemp, *Trends in Information Technology Law: Looking Ahead to 2014*, KEMPLITTLE, http://www.kemplittle.com/site/articles/kl_bytes/Trends_in_Information_Technology_Law_Looking_Ahead_to_2014 (last visited Feb. 15, 2014).

[169] *Id.*

Internet or otherwise, may undermined or reduce the effectiveness for surveillance in video games. This is especially true when there is no evidence that these surveillance programs have had any effect in deterring or preventing terrorism or crime.[170]

It is not all bad news for those who enjoy playing video games. A report by Benjamin Engelstatter of the Centre for Economic Research, Scott Cunningham of Baylor University, and Michael Ward of the University of Texas, have suggested that an increase in sales of either violent or non-violent crime can be associated with a decrease in violent and non-violent crime.[171]

Since the Supreme Court has not addressed many of the issues facing online gaming and virtual worlds concerning privacy, it is not clear whether gamers should have expectation of privacy from government intrusion. While many parts of the online game itself maybe public, there are many aspects of online video games that are private or appear to be private. It is hard to justify an expectation of privacy when the corporation that runs the game servers and systems claims ownership of all the personal information a player provides. The corporation also claims ownership of all in game actions and materials and which could compliment self-regulation of online games. Since it is also unclear the extent to which government and private corporations share information, there is no way to verify if the government has already viewed or accessed a player's personal information.

Anonymity in online games has its perks and its down sides. Anonymity allows for self-expression and self-discovery without fear of persecution. However anonymity can lead to

---

[170] *NSA Documents*, *supra* note 3.

[171] Benedict Carey, *Shooting in the Dark,* N. Y. TIMES (Feb. 12, 2013), *available at* http://www.nytimes.com/2013/02/12/science/studying-the-effects-of-playing-violent-video-games.html?pagewanted=1&_r=4&ref=science.

cheating. Additionally, anonymity can allow criminals and terrorists to act and communicate without the possibility of government supervision. Additionally, despite any expectations there are no specific laws or rulings by the Supreme Court that give gamers an expectation of privacy with in the games that they play. Furthermore, there are no clear rules as to what parts of a video game experience may be protected. Are single player experiences more private than multiplayer experiences? Do they deserve the same protections simply because they are played using the same hardware and software? Privacy concerns grow as technology grows and develops.

The leaked NSA documents most likely only describe the tip of the iceberg in government surveillance capabilities both in online games and on the Internet at large. But since the government has not been transparent about its data collection capabilities, it remains unclear what laws if any the government has violated. And thus, some may find it upsetting that despite the revelation that government agents are playing video games with you, they may not have violated any privacy laws. However, it is possible that many online video game players may now have a greater interest in a job with the FBI or NSA. In conclusion, a gamer does not have expectation of privacy, but there should be more transparency for the government's actions.

SYRACUSE JOURNAL OF SCIENCE & TECHNOLOGY LAW

VOLUME 31 2014-2015 ARTICLE 5, PAGE 132

I KNOW WHO YOU ARE AND I SAW WHAT YOU DID

[SOCIAL NETWORKS AND THE DEATH OF PRIVACY]

Justin McHugh[1]

Citation: LORI ANDREWS, I KNOW WHO YOU ARE AND I SAW WHAT YOU DID (Free Press ed., 2011).

Relevant Legal and Academic Areas: Constitutional Law, Intellectual Property Law, Tort Law, Internet Law, Criminal Law, Privacy, Social Media, Facebook, Twitter, Google, YouTube, and Myspace.

Summary: *I Know Who You Are And I Saw What You Did [Social Networks and the Death of Privacy]* is a book pertaining to the Internet and specifically social media. The book describes the downward spiral that social media is having on society and the desperate need for change. Sadly, the law has not yet caught up with the ever changing technology and changings in social media. Every day the Internet and specifically social media is encroaching on our fundamental rights of expression and speech. Social media which was once a tool to expand freedom of expression has now turned into a tool of restriction. Internet and more specifically social media users need to wake up and take action before the Internet completely restricts their fundamental rights of expression and speech.

About the Author: Lori Andrews is a law professor that has focused her career on Law and Technology. She has been published numerous times and has often been a guest on *Oprah, 60 Minutes,* and *Nightline*.[2] Lori Andrews is a very influential lawyer who has used her expertise in Law and technology to advice the United States government on many issues pertaining to the ethical and legal issues surrounding the ever advancing technology that we use every day.

[1] Syracuse University College of Law, Juris Doctor expected 2015.

[2] LORI ANDREWS, I KNOW WHO YOU ARE AND I SAW WHAT YOU DID (Free Press ed., 2011).

I. INTRODUCTION

In this section the background of how social media, specifically Facebook, and the Internet track and use our information to market us products and develop an unrealistic model of our real selves.

A. Facebook Nation

Since the creation of Facebook, people have been flocking to social media to have their voices heard. Facebook now has over 750 million members making it the "third largest nation in the world."[3] With so many followers, Facebook has essentially become its own nation with its own followers, financial system, legal system, and relationships with fellow real world nations.[4] Just like with any nation, there are issues of privacy and governmental intrusion into people's lives. Generally, Facebook and the Internet have never given great reverence to users' privacy. Instead, Facebook and sites like Spokeo continue to collect data on people and sell it to the highest bidder.[5] Spokeo and Facebook are a part of a "multibillion-dollar industry of data aggregators."[6] These companies take Internet users data, bundle it up into neat little packages, and sell it to all sorts of interested third parties.[7] Advertising agencies, businesses, and

[3] ANDREWS, *supra* note 2, at 1.

[4] *Id.* at 2.

[5] *Id.* at 11.

[6] *Id.*

[7] *Id.*

government agencies can all benefit from the research and use of this data.[8] Advertising agencies can develop more narrowly tailored marketing strategies to get individuals to buy things that they do not really need.[9] Businesses can perform intrusive background checks on potential employees.[10] Lastly, the government or big brother can keep a better eye on us with promises of better security and protection.[11] The true repercussions of the continued sale of our search histories and Internet use are the loss of our privacy. Sadly, one judge even went as far to say that once you start using Internet services, "the right to privacy is lost, upon your affirmative keystroke."[12]

Social networks have the ability to bring a vast array of potential benefits such as being able to keep in touch with friends and family, stay up to date with the news, and interact with and be heard by the government and politicians, but at what cost?[13] People have been attracted to social media sites like Facebook so that they can express their ever evolving social self.[14] What most users fail to realize is that their expressions and opinions are being used by businesses to turn a profit. People started using Facebook and the Internet as a way to freely express their beliefs and values while interacting with other like-minded individuals.[15] "But unless people's rights [to privacy] are protected, social networks [and the Internet] will [only] serve to narrow

---

[8] ANDREWS, *supra* note 2, at 11.

[9] *See id.*

[10] ANDREWS, *supra* note 2, at 11.

[11] *Id.*

[12] *Id.*

[13] *Id.* at 12-13.

[14] *Id.* at 13.

[15] ANDREWS, *supra* note 2, at 13.

people's behavior and limit their opportunities, rather than expand them."[16] The continued intrusion and eventual elimination of Internet user's privacy rights will only bring negative repercussions. There have already been specific examples seen where employees or potential employees have been fired or denied a job opportunity because of their private actions online.[17] If Facebook and Internet users do not smarten up and take charge of their privacy rights, they may soon find that nothing in their lives is private anymore.

B. George Orwell…Meet Mark Zuckerberg

From the moment we log onto the Internet our every move is being tracked, detailed, and stored by "data aggregators" who then use this supposedly private information to tailor marketing campaigns and ads directly to our likes and dislikes.[18] The reason for this ever increasing desire for our private information is known as "behavioral advertising".[19] The Federal Trade Commission has categorized "behavioral advertising [as] the tracking of consumers' online activities in order to deliver tailored advertising."[20] Through the use of behavioral advertising, businesses are better able to target individuals and market specific products to them that they are more likely to buy according to their Internet footprint.[21] This type of narrowly targeted advertising has led to a tremendous increase in profits for the businesses that practice

---

[16] *Id.*

[17] *See id.*

[18] ANDREWS, *supra* note 2, at 18.

[19] *Id.*

[20] *Id.*

[21] *See id.*

it.[22] Facebook is one of the most well-known businesses that mine our personal information and sell it to third party companies who use the information in their behavioral advertising strategies.[23] One of the negative effects of companies like Facebook collecting and selling our personal information that is only now starting to be fully understood has become known as "weblining."[24] "Weblining" was developed to describe the negative effects that our digital trails online can have on our potential economic and social opportunities.[25] There can be serious side effects based solely on the interactions people have online. Depending on what people do online can severely affect the opportunities that will be offered to them.[26] These missed opportunities can come in the form of missed discounts, higher interest rates, and decreased credit lines to name a few.[27]

One of the major downside to weblining is that it can literally narrow the type of information that we see and access online.[28] Narrowing the information we see and have access to online can have a direct effect on the way we perceive the world around us. Eli Pariser summed it up best when he stated that "Ultimately, democracy works only if we citizens are capable of thinking beyond our narrow self-interest. But to do so, we need a shared view of the world we cohabit."[29] Having our interests dictate what we see online deprives us of seeing ideas

[22] ANDREWS, *supra* note 2, at 18.

[23] *Id.* at 19.

[24] *Id.* at 19-20.

[25] *Id.* at 20.

[26] *Id.* at 20-21.

[27] ANDREWS, *supra* note 2, at 20-21.

[28] *Id.* at 21.

[29] *Id.*

from a different perspective. Ultimately, this online personalization can cause us to become more narcissistic and narrow minded individuals.[30]

Online personalization, curtailing, and narrowing the type of information we see online are based on the websites we visit and the way third parties track our movements online.[31] Companies like Comcast use tracking tools to follow us online and store data on our habits and preferences.[32] This surveillance information is used to create an image of a person that will better help third parties market and sell products to them.[33] Data mining is big business and helps companies to develop an image of your online self, known as your "second self."[34] The problem is that this second self is usually distorted and not accurate of the user it is trying to portray.[35] This distortion comes from the fact that the same user does not always use the same computer or may be searching online for someone other than themselves.[36] Collectors of our online data do not account for all the potential variables that may affect how we come across online. One consequence of this is that behavioral advertisers will use distorted online tracking information to predetermine what we see online.[37] As previously mentioned, this can lead to less freedom online and a more narrow view of what we see and are able to interact with online.[38]

---

[30] *See id.*

[31] ANDREWS, *supra* note 2, at 21-23.

[32] *Id.* at 22.

[33] *Id.* at 22-25.

[34] *Id.* at 28.

[35] *Id.* at 18-29.

[36] ANDREWS, *supra* note 2, at 28-29.

[37] *Id.*

[38] *Id.* at 29.

What is even more horrifying is that "[o]ur digital doppelgangers are directing our futures and the future of society" through distorted images that narrow our opportunities and proliferate stereotypes.[39]

C. Second Self

The image that we create of ourselves through our use of social media is often distorted due to the lack of regulations on the collection of our personal data and the intrusions into our privacy. The Federal Trade Commission is only now starting to create new ways to regulate the way our information is collected and used to market us products.[40] There are numerous federal laws that can be applied to the collection of online data in order to protect the privacy of individuals. The Computer Fraud and Abuse Act, the Stored Communications Act, and the Wiretap Act have all been used in the past to protect individual's private information.[41] The problem is that many courts have inadvertently created loopholes that privilege data aggregators over the individual's data that they are collecting.[42] In the landmark case *In re DoubleClick*, a New York federal judge found that the "data aggregator's intent was not to commit a tort or a crime, but rather to make a lot of money so its activities were permissible."[43]

Despite the loopholes developed from some unsavory federal court decisions, there is still hope for bringing data aggregators to justice for stealing personal information. The Federal

---

[39] *Id.*

[40] *Id.* at 47.

[41] ANDREWS, *supra* note 2, at 43.

[42] *Id.*

[43] ANDREWS, *supra* note 2, at 44.

Trade Commission has been the leading advocate for protecting consumer's rights from social networks, advertisement agencies, and data aggregators.[44] The FTC was granted the power to protect consumers against "unfair or deceptive acts or practices."[45] Through the Federal Trade Commission, individuals can file complaints against businesses for their deceptive practices. Beginning in the early 2000s, many individuals started to file complaints against data aggregators for deceptively acquiring their personal information from the Internet.[46] The Federal Trade Commission has gone after large companies such as Google, Facebook, and many other data aggregators and has forced them to implement some privacy changes.[47]

What most people fail to realize is that most companies have free rein to track and collect our personal information. Before we can develop a way to protect our privacy and second selves online, people need to become aware of how much of their personal information is actually being stolen.[48] Knowing how significantly and readily individuals' rights are being trampled on while using the Internet may be the catalyst needed for change.[49]

II. ANALYSIS

This section describes how our fundamental rights are being encroached on and an analysis of what freedom of speech and expression actually means.

---

[44] *Id.* at 46.

[45] *Id.*

[46] *Id.*

[47] *Id.*

[48] ANDREWS, *supra* note 2, at 48.

[49] *See id.*at 47-48.

A. Technology and Fundamental Rights

Technology is continually being used to intrude into our own personal lives.[50] These intrusions are happening without our consent or our knowledge.[51] The key to protecting our fundamental rights of privacy must come from knowledge and people spreading the word of exactly how our rights are being trampled on.[52] As more and more people realize how our fundamental rights are being encroached on, there will be a greater outcry for protection.[53] Eventually, the law will catch up with how technology is stealing our freedom away and selling it to the highest bidder.[54] Until that day, we must be wary of our actions online and the possible repercussions they will have on our future selves. Finding a balance between wanting to stay connected with our friends and family and our ever expanding social network versus the loss of our fundamental rights is a good place to start.[55]

B. The Right to Connect

Groups are using social media such as Twitter and Facebook to coordinate and plan protests.[56] Specifically, social media was used to help coordinate the protests in Egypt.[57]

---

[50] *See* ANDREWS, *supra* note 2, at 49.

[51] *Id.*

[52] *Id.* at 51.

[53] *Id.*

[54] *Id.* at 51-53.

[55] ANDREWS, *supra* note 2, at 57-59.

[56] *Id.* at 61.

Essentially, young adults were able to organize protests and rallies all through the use of Facebook pages and Twitter accounts.[58] The potential for using social media as a medium to promote democracy and freedom became quite apparent when protests began taking place throughout Egypt.[59] It was not long before former President Hosni Mubarak saw this potential threat to his dictatorship and had the Internet shut down all throughout Egypt.[60] But by now it was too late as protestors continued to take to the streets and alleyways to proclaim their abhorrence of former President Hosni Mubarak's authoritarian practices.[61] It is ironic how social media sites are helping to promote democracy at the same time as they are taking away our freedoms.

C. Freedom of Speech

The United States Constitution generally protects freedoms of speech and expression.[62] However, when it comes to what is posted on social media sites, it would seem that for some reason these protections do not apply.[63] Students and teachers alike have been reprimanded for pictures or comments they have posted on social media websites.[64] In some of the more bizarre cases, students have been expelled and teachers have been fired for what seems to be very minor

[57] ANDREWS, *supra* note 2, at 61.

[58] *Id.* at 61-62.

[59] *Id.* at 61-63.

[60] *Id.* at 61-62.

[61] *Id.* at 62.

[62] ANDREWS, *supra* note 2, at 76.

[63] *Id.*

[64] *Id.*

offenses.[65] One student was expelled for posting comments about the poor conditions of his school on his Facebook account.[66] In another strange example, a teacher was expelled when a picture of her with a glass of wine was posted on Facebook from years ago.[67] In a Country that celebrates freedom of expression and speech, it would seem that these fundamental rights are somehow lost when using the Internet.[68] The entire concept of democracy is based on the freedom to express oneself and ideas while not encroaching on another's freedoms.[69] If freedoms of speech and expression are taken away what will be left of democracy? The author argues that people should be free and enabled to express themselves unless that speech is meant to cause imminent societal harm.[70] Expressing one's likes and dislikes is a basic staple of democracy that can help enable societal change where needed.[71] Social media was meant to enable users to express their ideas and beliefs. Instead of expanding freedoms of speech and expression, it would seem that individuals are losing these fundamental rights.[72]

D. Lethal Advocacy

Numerous individuals are turning to social media to express their most intimate secrets and feelings. Nadia Kajouji, an 18-year-old student at Carleton University in Ontario, Canada

[65] *Id.* at 76-77.

[66] *Id.* at 76.

[67] ANDREWS, *supra* note 2, at 76-77.

[68] *Id.* at 77.

[69] *Id.* at 90.

[70] *Id.*

[71] *Id.*

[72] ANDREWS, *supra* note 2, at 89-90.

used social media to describe her downward spiral into depression.[73] Through her use of social media sites, Nadia was able to find someone whom she thought really understood the type of depression she was going through.[74] On a social network, Nadia met a young American nurse, Cami, who claimed to be suffering from depression as well.[75] Nadia believed that she had finally found someone who understood what she was going through, in reality this could not have been further from the truth.[76] The truth was that Cami was not the name of a young American nurse suffering from depression.[77] Cami was a "46-year-old man, William Francis Melchert-Dinkel, who got his sick kicks out of attempting to convince young women to slash their wrists or hang themselves in front of a webcam so he could watch."[78] Cami, who was actually William Francis Melchert-Dinkel, had convinced Nadia that the only way to release herself from her depression was to commit suicide.[79] On March 10, 2008, Nadia drowned herself in Ottawa's Rideau River.[80]

Celia Bay, a retired school teacher suffering from depression had found Cami on a similar social networking site.[81] After reading some of Cami's posts to children suffering from

[73] *Id.* at 91.

[74] *Id.* at 92.

[75] *Id.*

[76] ANDREWS, *supra* note 2, at 92.

[77] *Id.*

[78] *Id.*

[79] *Id.* at 92-93.

[80] *Id.* at 93-94.

[81] ANDREWS, *supra* note 2, at 92-93.

depression, Celia realized that something was wrong.[82] Cami, a.k.a. Melchert-Dinkel, had been telling depressed children that he would enter into suicide pacts with them, where they would both kill themselves together on web camera.[83] Celia brought all of the evidence and suspicions she had gathered on Cami, whom she believed to be Melchert-Dinkel, to the police.[84] When the police finally investigated Celia's claims, they discovered that Cami was in fact Melchert-Dinkel and had pressured dozens of people into committing suicide, including Nadia.[85]

Nadia's parents wanted Melchert-Dinkel to be brought to justice for his connection to Nadia's suicide.[86] However, many places will not hold a person liable for another's suicide unless he had provided the physical means by which Nadia killed herself or participated in the physical act of Nadia killing herself.[87] Melchert-Dinkel argued that he had neither of the actions required for him to be charged with assisting in Nadia's suicide.[88] Furthermore, Melchert-Dinkel argued that his words were protected under the First Amendment.[89] However, under the Constitution the government can penalize speech on the basis that it will incite or cause imminent harm to another individual.[90] In order to prosecute Melchert-Dinkel, a judge would

---

[82] *See id.*at 93.

[83] ANDREWS, *supra* note 2, at 93.

[84] *Id.* at 93-94.

[85] *Id.*

[86] *Id.* at 94.

[87] ANDREWS, *supra* note 2, at 94.

[88] *Id.*

[89] *Id.*

[90] *Id.* at 95.

have to find that his chat room conversations went beyond normal speech and incited imminent harm or danger.[91]

Judge Neuville rejected Melchert-Dinkel's First Amendment argument to free speech and pointed out that the First Amendment is not absolute.[92] Furthermore, Judge Neuville pointed out that Melchert-Dinkel's "encouragement and advice imminently incited the suicide of Nadia" and labeled his advice as "lethal advocacy."[93] Judge Neuville compared Melchert-Dinkel's words to the specific category of unprotected speech known as "fighting words" and "imminent incitement of lawlessness."[94] In May 2011, Judge Neuville levied a very peculiar sentence on Melchert-Dinkel.[95] Melchert-Dinkel would serve 320 days in prison, "plus an additional two days on the anniversaries of both victims [Nadia and Mark Drybrough] each year until 2021."[96]

This particular case is a warning of the possible harms that can be perpetuated through social media sites. In order for justice to be brought to the Web, freedom of speech needs to be limited when it is likely to cause imminent harm to another individual.[97] The author proposes that these limits should not only apply to the individuals on the social networks, but "to any social networks or websites that act as co-conspirators."[98]

---

[91] *Id.*

[92] ANDREWS, *supra* note 2, at 96.

[93] *Id.*

[94] *Id.*

[95] *Id.* at 97.

[96] *Id.*

[97] ANDREWS, *supra* note 2, at 110.

[98] *Id.*

E. Privacy of Place

In another bizarre incident, Lower Merion School District had issued 2,300 free laptops to its teachers and students.[99] Unbeknownst to the students or teachers, the free laptops were transmitting screenshots and pictures to the School District's Information Services Department for review.[100] When students and teachers found out that they were being spied on in their homes, they were furious.[101]

Blake, one of the students who had been spied on, along with his parents found out the hard way that no federal laws have caught up with the regulation of social networks and digital devices.[102] U.S. Attorney Zane Memeger specifically stated, "For the government to prosecute a criminal case, it must prove beyond a reasonable doubt that the person charged acted with criminal intent. We have not found evidence that would establish beyond a reasonable doubt that anyone involved had criminal intent."[103] With criminal prosecution unlikely to happen, Blake's family decided to take their case to the civil courts.[104] Three months after Blake's lawsuit had been filed, the school district finally agreed to stop the remote activation of student laptops.[105] Additionally, the district promised to destroy all of the photos that had been taken after the

---

[99] *Id.* at 111.

[100] *Id.*

[101] *Id.* at 111-12.

[102] ANDREWS, *supra* note 2, at 113.

[103] *Id.*

[104] *Id.*

[105] *Id.* at 115.

students and their parents had a chance to look at them.[106] In October 2010, months after the lawsuit had been filed, the school district decided to settle the lawsuits outside of court.[107]

This case is a prime example of how laws can lag behind technological innovation. Privacy laws need to be updated in order to protect individuals in their homes from remote spying through electronic devices. Author Lori Andrews, advocates for declaring a right to privacy while using social networks in order to protect our privacy from the intrusions of third parties.[108]

F. Privacy of Information

Employers, schools, and many other institutions are continually seeking more information from social media sites in order to make more informed decisions about people.[109] However, the small glimpses of an individual's life that these social networking sites can offer are causing the proliferation of false and misleading judgments.[110] Leaks from social media sites have "led to people divorcing, being fired, being denied admission to college, and committing suicide."[111]

---

[106] ANDREWS, *supra* note 2, at 115.

[107] *Id.* at 115-16.

[108] *Id.* at 118-19.

[109] *Id.* at 122.

[110] *See id.* at 122-23.

[111] ANDREWS, *supra* note 2, at 122.

In one particularly intrusive and saddening case, the gory images of an 18-year-old girl in a fatal car accident spread across the Internet causing irreparable harm to the family.[112] The gruesome pictures disbursed across the Internet after a dispatcher at the precinct that handled the accident, sent the pictures to his private email.[113] Unable to find peace and escape the gruesome pictures, the girl's parents filed a lawsuit against the California Highway Patrol that managed the accident.[114] The case went all the way to the California Court of Appeals before the officers were found to have violated their fiduciary duties to the family.[115] The California Court of Appeals had found that the officers handling the accident owed the young girl's family a duty of care not to place the accident's photos on the Internet.[116] The one positive thing to come out of this case was that the gate had now been open for legal action in future cases involving the invasion of privacy connected with the Internet.[117] Private images such as the aforementioned deceased girl's pictures should not be allowed to be disseminated without legal repercussions. Recognizing an individual's legal right to privacy could help prevent future dissemination of private information.[118]

G. FYI or TMI?: Social Networks and the Right to a Relationship with Your Children

Social media is changing the way courts and investigators gather information.[119] Postings on social media sites are being used as evidence in custody proceedings and divorces.[120] An American Academy of Matrimonial Lawyers poll found that 81% of divorce attorneys have seen an increase in the use of social networking evidence when couples divorce.[121]

---

[112] *See id.* at 133-34.

[113] ANDREWS, *supra* note 2, at 133.

[114] *Id.* at 134.

[115] *Id.*

[116] *Id.*

[117] *Id.*

[118] *See* ANDREWS, *supra* note 2, at 135.

[119] *Id.* at 137.

[120] ANDREWS, *supra* note 2, at 137.

[121] *Id.*

Attorneys involved in custody battles are also seeing a significant increase in the use of social networking posts as evidence in cases.[122] Both men and women are losing custody of their children due to the irresponsible posts they make on their social media websites.[123] Courts are continually admitting evidence from social networks to help determine which parent will retain child custody.[124] Evidence such as pictures of parents drinking on Facebook are being used to argue that parents are unfit to care for their children.[125] The use of social network posts should only be used when they are directly related to the care of a child.[126] The overzealous use and magnification of innocent postings can be used to prejudice a judge against an otherwise fit parent.[127]

Parenthood is often considered as one of the "basic civil rights of man."[128] Courts have continually reaffirmed that a parent has a fundamental right to determine how to raise their own child.[129] If courts are allowed to pry into a family's home life through the use of social networking sites, prejudices can form and the inappropriate denial of parental rights can be proliferated.[130] Courts have to be careful that they do not unduly prejudice parents when

---

[122] *See* ANDREWS, *supra* note 2, at 137-40.

[123] *Id.*

[124] ANDREWS, *supra* note 2, at 141.

[125] *Id.*

[126] *Id.*

[127] *Id.*

[128] *Id.* at 140.

[129] ANDREWS, *supra* note 2, at 140.

[130] *Id.* at 140-41.

evaluating social posts as evidence.[131] Allowing social posts as evidence in custody battles should be admitted only when there is a direct correlation between the post and the best interest of the child involved.[132]

H. Social Networks and the Judicial System

Judges, lawyers, and jurors alike are all increasingly using social networking sites to discuss cases and research information.[133] In 2008, studies showed that only 15% of attorneys used social networking sites.[134] Two years later, more than 56% of attorneys had social networking profiles.[135] The increased use of social network sites by attorneys and judges have in some cases led to suspicions of prejudice and conflict of interests.[136] In 2009, Judge Saffold was removed from a case when it was discovered that she had potentially made prejudicial statements against an attorney in a case she was presiding over.[137]

Jurors' use of social networking sites have also increasingly led to mistrials and overturned judgments.[138] In 2009, a single court had 600 potential jurors dismissed when they

---

[131] *Id.* at 141.

[132] *Id.*

[133] *See* ANDREWS, *supra* note 2, at 149-59.

[134] ANDREWS, *supra* note 2, at 153.

[135] *Id.*

[136] *See* ANDREWS, *supra* note 2, at 149-59.

[137] ANDREWS, *supra* note 2, at 151.

[138] *Id.* at 154.

had mentioned that they had done prior research about individual cases.[139] Technology and social networking sites can allow jurors to easily gain access to outside information which can prevent a defendant from a fair trial.[140] In one particular case, a juror used his smartphone to look up a key legal term in a manslaughter trial.[141] Only after the defendant had been convicted, did the external research done by the juror emerge.[142] The defendant was granted a new trial with the appellate court stating,

> "Although here we confront new frontiers in technology, that being the instant access to a dictionary by a smartphone, the conduct complained of by the appellant is not at all novel or unusual. It has been a long-standing rule of law that jurors should not consider external information outside the presence of the defendant, the state, and the trial court."[143]

Judges and lawyers have long been held responsible when using social networks in ways that can negatively impact cases.[144] Jurors have also begun to be penalized for ignoring instructions and conducting external research.[145] In order for all people to be afforded fair trials,

---

[139] *Id.*

[140] *Id.*

[141] *Id.* at 156.

[142] ANDREWS, *supra* note 2, at 156.

[143] ANDREWS, *supra* note 2, at 156.

[144] *Id.* at 158.

[145] *See* ANDREWS, *supra* note 2, at 158-59.

judges, lawyers, and jurors must be disciplined for prejudicial use of social networks and technology.[146]

I. The Right to a Fair Trial

The increased use of social network sites as evidence in criminal cases has many people questioning the validity of that evidence. In Martinsburg, West Virginia, a robber had checked his Facebook on the victim's computer and then left the computer with his Facebook page still open.[147] Officers were easily able to identify and find the suspect from his Facebook page.[148] In this case in turns out that the use of a social network site as evidence was beneficial. However, there are many cases where social networking sites have been used to frame the wrong person or create prejudicial thoughts against potential suspects.[149]

"A [recent] survey by the International Association of Chiefs of Police of 728 law enforcement agencies … found that 62% of the agencies used social networks in criminal investigations."[150] In some of the more bizarre cases, thieves have been identified after having posted pictures of themselves on social networking sites with the stolen goods.[151] Additionally,

[146] ANDREWS, *supra* note 2, at 159.

[147] *Id.* at 161.

[148] *Id.*

[149] *See id.*

[150] ANDREWS, *supra* note 2, at 162.

[151] *Id.*

Robert Petrick's conviction for murdering his wife was based off evidence gleaned from his computer's search history on how to kill his wife and where to dump the body.[152]

Despite the many cases that have been solved through the use of social networking sites, the current uses of these sites tramples on individuals' Fourth Amendment rights.[153] The Fourth Amendment was meant to protect individuals' privacy and to prevent unreasonable searches and seizures of property.[154] Officers need some individualized suspicion that an individual has committed a crime before they can search them.[155] The use of aggregate data from social networking sites completely sidesteps the element of individualized suspicion and can cause discrimination.[156] In a particular case, an African American man was searched at an airport based on aggregate data that shows drug runners carry little luggage and appear to be nervous.[157] The man was found to have drugs on him, but a dissenting judge argued that the search was improper.[158] The judge proclaimed that he himself is sometimes agitated when he flies, but he is never searched because he is white.[159]

Judges, prosecutors, and officers need to be careful when verifying the validity of information obtained on social networking sites. The author argues that social networks should not be accessed for evidence unless there is an individualized suspicion that that person has

[152] *Id.*

[153] *See* ANDREWS, *supra* note 2, at 162-63.

[154] ANDREWS, *supra* note 2, at 163.

[155] *Id.*

[156] *Id.*

[157] *Id.*

[158] *Id.*

[159] ANDREWS, *supra* note 2, at 163.

committed a crime.[160] Furthermore, when judges allow social networking evidence to be admitted, the reliability, authenticity, and relevance of the evidence must be taken into consideration.[161]

J. The Right to Due Process

The thoughtless speed in which social networking sites change their privacy policies has caused harm to many of their users.[162] When Facebook changed its privacy policies, many Iranian-Americans who opposed Iran's policies received threats.[163] The families of these Iranian-Americans still in Iran were arrested and also threatened.[164]

Currently, users of social networking sites like Facebook do not receive adequate warning of the repercussions their postings can cause.[165] Additionally, users of social networking sites are not receiving adequate notices of when these sites change their policies.[166] Users on social networking sites should be told well in advance of policy changes that could potentially affect their lives and privacy.[167] Furthermore, no policy change should be

[160] ANDREWS, *supra* note 2, at 171.

[161] *Id.*

[162] *See id.*at 173.

[163] ANDREWS, *supra* note 2, at 173.

[164] *Id.*

[165] *Id.* at 175.

[166] *Id.* at 182-83.

[167] *Id.* at 182.

implemented without a user's explicit consent and knowledge of what the policy changes entail.[168]

III. RECOMMENDATIONS

The demand for greater privacy and protection on social networking sites will lead to better legal regulation of the Internet.

A. Slouching Towards a Constitution

The outcry for greater privacy comes as no surprise with the way social networking sites currently mine and sell our data without users' consent. Social networking sites such as Facebook provide users with ample opportunities to express one's individuality and thoughts.[169] However, without some more regulation on how these sites use our data, the value of joining these sites will be greatly reduced.[170] As more users become aware of how their privacy is being taken away, there will hopefully be a greater demand to take back their fundamental rights. Social network and Internet users need to band together and apply our Constitutional rights of privacy and expression to not only offline actions, but to online activities as well.[171]

---

[168] ANDREWS, *supra* note 2, at 182.

[169] *See id.*

[170] ANDREWS, *supra* note 2, at 188.

[171] *See id.*

IV. CONCLUSION

In order to protect our fundamental rights of privacy and freedoms of expression and speech, Lori Andrews purposes that all Internet and social networking users adopt a Social Network Constitution.[172] Among the numerous principles and ideologies described throughout her book, the most important points can be summed up in the ten rights and freedoms of her Social Network Constitution.[173]

The first right is the right to connect.[174] Lori argues that all individuals have a right to connect over the Internet without undue influence from the government.[175] Second, just like in the First Amendment, all individuals have the right to free speech and freedom of expression as long as it does not encroach on the rights of others.[176] Third, users of social networking sites should have the right to privacy of place and information while using those websites.[177] Fourth, users should have the right to have their thoughts and expressions kept private when posting on social sites.[178] Fifth, the image or second self that is created from the information posted on the Internet should be the sole possession of the individual user who created that image.[179] Sixth, evidence should only be collected from social networking sites when there is an individualized

[172] *See* ANDREWS, *supra* note 2, at 189

[173] *Id.* at 189-91.

[174] ANDREWS, *supra* note 2, at 189.

[175] *Id.*

[176] *Id.*

[177] *Id.*

[178] *Id.* at 190.

[179] ANDREWS, *supra* note 2, at 190.

suspicion that a user has committed a crime.[180] Seventh, all defendants in court should be judged by an unbiased group of their peers.[181] Eighth, users of social networking sites should be given advance notice of site policy changes.[182] Ninth, all users of social networking sites shall not be discriminated against because of data collected on them through networking sites.[183] Lastly, all social network users shall have the right to associate with whomever they please and to have those associations kept private.[184]

[180] *Id.*

[181] *Id.* at 191.

[182] *Id.*

[183] *Id.*

[184] ANDREWS, *supra* note 2, at 191.

SYRACUSE JOURNAL OF SCIENCE & TECHNOLOGY LAW

VOLUME 31 2014-2015 ARTICLE 6, PAGE 158

TO PROTECT AND SERVE, BUT NOT DRIVE: POLICE USE OF AUTONOMOUS VEHICLES

Geoffrey Wills[1]

ABSTRACT

This paper will discuss the rapidly developing technology of autonomous vehicles and the legal ramifications of police departments across the country using them. This note will discuss that when autonomous vehicles become commercially viable and available, law enforcement could use these autonomous vehicles, allowing their officers to use their time more efficiently due to autonomous vehicles taking on the load of traffic patrol. This paper also discusses how autonomous vehicles used for law enforcement will result in an increased level in officer safety. Additionally, the argument will be made that these vehicles will result in less officer discretion and subjectivity, and will be a better vehicle for legally permissible evidence gathering.

[1] Mr. Wills is a student at Syracuse University College of Law, Juris Doctor expected May 2015. Mr. Wills wishes to express his great appreciation for the advice and guidance provided by Professor Lauryn Gouldin in the development of this note.

INTRODUCTION

Images of *Knight Rider*, *Herbie the Love Bug*, or HAL from *2001: A Space Odyssey* might be the first thing people think of when discussing artificial intelligence and self-driving vehicles, but that is quickly changing. While a self-driving car used to be just a pipe dream, an ever-increasing number of car manufacturers are taking off with the concept, but technology still needs to be developed and perfected before autonomous vehicles can be mass-produced and used for daily use. Currently, fully autonomous vehicles have traveled safely at speeds up to 31 miles per hour.[2] Car manufacturers including General Motors, Audi, Nissan, and BMW all expect fully autonomous, driverless cars to be in dealership showrooms by 2020.[3]

As curiosity and demand for these vehicles increase, the need for understanding how the law applies to them also increases. This leads to an important question that could have major implications for the future: what if police departments use this technology to patrol the streets and keep cities safe? This note will analyze and attempt to answer these questions, and will also discuss the technological history of autonomous vehicles, as well as the evolution of applicable law that will dictate the use of these "driverless" cars. This essay will be broken down into several parts. Part I will give a brief rundown of how autonomous vehicle technology works. Part II will discuss the legality of vehicle automation and the technologies inside the car, including how many of these technologies not only currently exist, but are legally permissible for crime prevention and surveillance purposes. Part II will also look at social acceptability of autonomous

[2] Early prototypes, such as Volvo's autonomous vehicles, are expected to roll out as soon as 2014. Volvo's model has the capability to autonomously drive safely up to 31 miles per hour. Charles Duxbury & John D. Stoll, *Volvo Plans to Roll Out Self-Driving Cars in 2014*, WALL. ST. J. DRIVER'S SEAT BLOG (Dec. 3, 2012, 10:00 AM), http://blogs.wsj.com/drivers-seat/2012/12/03/volvo-plans-to-roll-out-self-driving-cars-in-2014/.

[3] Dan Bigman, *Driverless Cars Coming to Showrooms by 2020, Says Nissan CEO Carlos Ghosn*, FORBES (Jan. 14, 2013, 4:39 PM), http://www.forbes.com/sites/danbigman/2013/01/14/driverless-cars-coming-to-showrooms-by-2020-says-nissan-ceo-carlos-ghosn/.

vehicles patrolling the streets and enforcing laws. Finally, Part III considers how autonomous vehicles will have the capability to take subjectivity, discretion, and potential prejudice out of patrolling and traffic stops, as well as increasing officer safety and efficiency.

I. GETTING FROM POINT "A" TO POINT "B" WITHOUT HUMAN ASSISTANCE

The technology that an autonomous vehicle uses to get around without needing human control is not something that was created overnight. An autonomous vehicle is made up of many different technologies acting together, some of which have been around for decades, others of which have been developed in the last few years. Components like cruise control used in human-controlled vehicles have been around for over 50 years.[4] Other technologies, like front crash prevention and adaptive headlights, are recent innovations that are just now being seen as basic features in cars.[5]

To fully understand what "autonomous" means in the eyes of the law and government regulation, the United States Department of Transportation released a policy statement that categorized autonomous vehicles based on the amount of technology a vehicle uses.[6] These categories, or levels, go from level zero, where no automation is present, all the way to level four, "full automation," where the vehicle is designed to perform all safety-critical driving functions and monitor roadway conditions for an entire trip.[7] This type of design anticipates that

[4] U.S. Patent No. 2,519,859 (filed Aug. 11, 1950).

[5] *Crash Avoidance Technologies*, INS. INST. FOR HIGHWAY SAFETY, http://www.iihs.org/iihs/topics/t/crash-avoidance-technologies/topicoverview (last visited Feb. 13, 2014).

[6] Press Release, U.S. Department of Transportation Releases Policy on Automated Vehicle Development, NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., (May 30, 2013) *available at* http://www.nhtsa.gov/About+NHTSA/Press+Releases/U.S.+Department+Transportation+Releases+Policy+on+Automated+Vehicle+Development.

[7] *Id.*

the driver will provide destination or navigation input, but is not expected to control the vehicle at any time during the trip.[8] This level includes occupied and non-occupied vehicles, and safe operation rests solely on the automated vehicle system.[9] For purposes of this essay, any autonomous vehicle discussed for police use will be fully autonomous and non-occupied.

Autonomous vehicles go from destination to destination without human interaction by using a combination of sensors, ultrasound, radar, GPS units, and cameras.[10] Google's autonomous vehicle uses LIDAR, which consists of a constantly spinning unit that houses laser emitters and laser receivers.[11] 64 lasers and receivers are used to create a detailed map of the cars surroundings as it moves.[12] When the LIDAR is connected with the other components of the car with interconnected software, the data is compared with existing maps, allowing the vehicle to get around and avoid any differences in the data and the maps in the software, like people, other cars, or detours.[13] Much of the technologies used here are already in use on the road. Radar is used increasingly in vehicles for safety features like adaptive cruise control and blind spot monitoring.[14] Cameras are used for in-lane keeping systems.[15] Sensors are already used in anti-

[8] *Id.*

[9] *Id.*

[10] Henry Fountain, *Yes, Driverless Cars Know the Way to San Jose,* N.Y. TIMES (Oct. 26, 2012), http://www.nytimes.com/interactive/2012/10/28/automobiles/how-an-autonomous-car-gets-around.html?ref=automobiles.

[11] *Id.*

[12] *Id.*

[13] *Id.*

[14] *Id.* at 2.

[15] Fountain, *supra* note 10, at 2.

lock brakes and stability control systems.[16] GPS devices, whether they are part of the car or in a cell-phone, can already be found in just about every car on the road.[17]

II. LEGALITY AND SOCIAL ACCEPTABILITY OF AUTONOMOUS VEHICLES

A. Analyzing the Legal Aspects of Autonomous Vehicles

Autonomous technology is still relatively young, and the possible combinations of already available technologies with autonomous vehicles will be extremely sophisticated. Trying to completely foresee what will be considered a legal or illegal use and what the public perception of police use will be is a completely imprecise science, so past precedent will be used to try to estimate what might be permissible and socially acceptable.

In determining what might be legally permissible for police in using autonomous vehicles, the Fourth Amendment and its past interpretations will give particularly significant guidance. The Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[18]

According to the United States Supreme Court, police activity constitutes a search in one of two ways. The first method that constitutes a search is when law enforcement conduct intrudes upon an actual expectation of privacy, and one that society is prepared to recognize as

[16] *Id.* at 2.

[17] *Id.*

[18] U.S. CONST. amend. IV.

reasonable.[19] The second activity that the Supreme Court deemed to be a search under the Fourth Amendment is when law enforcement physically trespasses on the suspect's property conjoined with an attempt to find something or obtain information.[20]

The *Katz* test came out of a case in which the defendant was convicted of a crime after the government wiretapped a phone booth that the defendant frequented.[21] The court determined that since the phone booth was fully enclosed, it was considered to not be a public place.[22] *Katz* afforded an individual stronger privacy rights, but did imply that conversations in public would not enjoy the same privacy protections.[23] On this point, Justice Stewart noted, "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[24]

As police have used an increasing level of technology for surveillance, patrolling, and evidence gathering, the Supreme Court has had to decide what types of technology are permissible, as well as when they can be used. When determining whether or not certain technologies may be used for policing purposes, courts look to the commercial availability and general public use of such technology.[25] Assuming that autonomous vehicles become fully

[19] Katz v. United States, 389 U.S. 347, 361 (1967).

[20] *See* United States v. Jones, 132 S. Ct. 945 (2011).

[21] *See Katz*, 389 U.S. at 347.

[22] A modern-day example of this would be having a conversation on a cell phone and a police officer walks by. *Id.* at 352.

[23] *Id.*

[24] *Id.*

[25] Kyllo v. United States, 533 U.S. 27, 28 (2001).

regulated and become legally available at car dealerships across the country, allowing use of these vehicles for police use would be a safe conclusion to jump to. The main issue here though is not whether the actual car would be legally permissible. States have already incorporated legislation into their state regulations regarding autonomous vehicles, making it reasonably to assume that the addition of proper future federal regulation would likely create few obstacles to making fully-autonomous vehicles legal.[26] Instead, the main issue is whether the technology used *inside* the vehicle, like cameras, audio recorders, GPS devices, and potentially even thermal cameras would pose any Fourth Amendment problems. Surveillance cameras will be specifically addressed, since they will likely be the most used type of technology inside of an autonomous police vehicle.

The line of cases that have followed Katz have been decided so similarly that the issue may very well be settled, despite the fact that the Supreme Court has never specifically ruled on executive use of surveillance cameras.[27] These cases seems to have come up with a synthesized rule that almost any knowing exposure to a third party could defeat a claimed reasonable expectation of privacy.[28] A criminal that confides in a friend might not even be able to raise a claim for a reasonable expectation of privacy, because there is a risk that his companions may be

[26] NEV. REV. STAT. §482a (2012). Nevada's statute regarding autonomous vehicles require registration, licensing, and a certificate describing geographic locations that autonomous vehicles are allowed to travel. The language found here is significantly similar to the other motor vehicle provisions found in Nevada's statutory code. *See* NEV. REV. STAT. §482 (2012).

[27] *See* Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 19-20 (2008).

[28] In addition to the reasonable expectation privacy test in *Katz*, the Supreme Court has also kept historical distinctions in place, such as open fields, curtilage, and the home. *See generally* United States v. Dunn, 480 U.S. 294 (1987).

reporting to the police.[29] These decisions have given police tremendous power and ability to use technology to conduct surveillance on suspected criminal activity.

In *Knotts*, the court rejected the defendant's claim that using a GPS device amounted to a search.[30] The court reasoned that a vehicle has little capacity for escaping public scrutiny because it travels through public places where both occupants and its contents are in plain view.[31] Because possible visual surveillance by police could have revealed the same information that the GPS did, there was no reasonable expectation of privacy.[32] In what might amount to a significant understatement of future technology, the court also noted that nothing in the Fourth Amendment keeps the police from "augmenting the sensory faculties bestowed upon them at birth" with such enhancement that technology may afford them.[33] This could potentially give police departments the legal ability to fully equip autonomous vehicles with the most up to date surveillance equipment.

In *United States v. Karo*, the court found that government installation of a tracking device to monitor travel outside the home, where there is no reasonable expectation of privacy, was not a search, and did not afford the defendant any Fourth Amendment protections.[34] This decision reaffirmed the court's ruling in *Knotts*.

In *United States v. Jones*, the court reaffirmed its view that the Fourth Amendment provides no protection to activities conducted in public, but did decide that attaching a GPS

[29] United States v. White, 401 U.S. 745, 752 (1971).

[30] United States v. Knotts, 460 U.S. 276, 285 (1983).

[31] *Id*. at 281.

[32] *Id*.

[33] *Id*. at 282.

[34] *See* 468 U.S. 705 (1984).

device to the defendant's car amounts to a trespass of a constitutionally protected area.[35] This is technically distinguishable from the both *Knotts* and *Karo*, because the GPS devices in those cases were not directly attached to any of the defendant property. This could be used to allow autonomous police vehicles to use it's own GPS data to track a suspects travel without amounting to a trespass, and without needing a warrant for Fourth Amendment purposes.

Jones was decided 5-4, with all nine Justices concluding that the search was unconstitutional.[36] The disagreement among the court was a result of the fundamental reasoning behind the ruling. In a concurring opinion, Justice Alito disagreed with the trespass portion of the majority opinion, instead focusing on individual privacy rights.[37] Justice Alito opined that "short-term monitoring of a person's movements on public streets accords with expectations of privacy, but the use of *longer term* GPS monitoring in investigations impinges on expectations of privacy.[38] Alito reasoned that prolonged surveillance reveals every type of information about a person."[39]

Justice Alito's concurrence, had it received one more vote, would have held that monitoring every single movement of an individual's car for 28 days violated a reasonable expectation of privacy.[40] This would have more closely followed the lineage of Fourth Amendment jurisprudence following *Katz*.

---

[35] *See* 132 S. Ct. 945 (2011).

[36] *See id*.

[37] *Id.* at 957 (Alito, J., concurring).

[38] *Jones,* 132 S. Ct. at 964 (emphasis added).

[39] *See Id*.

[40] *Id.* at 957 (Alito, J., concurring). Alito did not specifically say what amount of time constituted a search, but four weeks surely crossed the line.

Along with potentially being able to pass any Fourth Amendment scrutiny, proponents of police use of autonomous vehicles should successfully be able to argue that the technology they use is already legal and in existence. Surveillance cameras have already been implemented in many cities around the United States, and have withstood Fourth Amendment challenges. For example, the Tenth Circuit held that cameras installed on telephone poles are not subject to Fourth Amendment scrutiny, because they "observe only what any passerby would easily have been able to observe."[41] Multiple cities around the United States have incorporated surveillance cameras into their police force in an attempt to better protect their citizens. Washington, D.C., Chicago, and Baltimore are all large cities that utilize surveillance technologies to monitor their cities.[42] These technologies mainly consist of cameras, but some have also incorporated facial recognition software into the video feed to look out for potential suspects.[43] The most significant and best example of surveillance camera use is in New York City.

New York City has partnered up with Microsoft to roll out a public surveillance device called the Domain Awareness System.[44] This system aggregates and analyzes information from around 3,000 surveillance cameras around the city and allows police to scan license plates, check criminal databases, and measure radiation levels, among other things.[45] The use of surveillance cameras has existed since the mid-1970's, when cameras were used for crime prevention and

[41] United States v. Jackson, 213 F.3d 1269, 1281 (10th Cir. 2000).

[42] *See* I. Bennett Capers, *Crime Surveillance, and Communities*, 40 FORDHAM URB. L.J. 959, 962-63 (2012).

[43] Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 MINN. L. REV. 407, 409 (2012).

[44] Joe Cascarelli, *The NYPD's Domain Awareness System is Watching You*, N.Y. MAG. DAILY INTELLIGENCER (Aug. 9, 2012, 8:50 AM) http://nymag.com/daily/intelligencer/2012/08/nypd-domain-awareness-system-microsoft-is-watching-you.html.

[45] *Id.*

detection in Times Square. Along with the new Domain Awareness System, there are enough surveillance cameras in lower Manhattan that if you were in a public space, the odds were "pretty good" you were being watched.[46] This might sound scary and create some apprehension, but these systems work. Surveillance equipment was one of the primary tools used in preventing terrorist attacks in Times Square, John F. Kennedy Airport, and in the Bronx in 2010.[47]

In addition to the massive surveillance systems that already exist, autonomous police vehicles would likely also use the federal government's Intelligent Transportation Systems initiative, which proposes a future where all cars use wireless technology to communicate with each other, as well as devices embedded in the road.[48] This data would include location and speed, as well as problems with the car's mechanics or registration.[49] Here, the potential for law enforcement is great. Traffic violations like speeding, running a stoplight, or even driving under the influence could be automatically and remotely enforced using the data generated.[50] Aside from law enforcement purposes, these systems also serve an important public policy: public safety.[51] Crashes could be significantly reduced through automated enforcement, because the proper intent of these systems is to reduce violations by modifying driving behavior.[52] This

[46] Bob Hennelly, *A Look Inside the NYPD Surveillance System*, WNYC NEWS (May 21, 2010), http://www.wnyc.org/articles/wnyc-news/2010/may/21/a-look-inside-the-nypd-surveillance-system.

[47] Chris Dolmetsch, *Cameras to Catch Terrorists Triple Since June in New York With Bomb Plots*, Bloomberg News (Nov. 13, 2010, 12:01 AM), http://www.bloomberg.com/news/2010-11-12/cameras-to-catch-terrorists-triple-since-june-in-new-york-with-bomb-plots.html.

[48] Elizabeth E. Joh, *Discretionless Policing: Technology and the Fourth Amendment*, 95 CAL. L. REV., 199, 200 (2007).

[49] *Id*.

[50] *Id.* at 221.

[51] *Id*.

[52] *Id*.

would create an additional connection between governmental autonomous vehicles and the surveillance infrastructure of any given city.

Due to the already existing use of surveillance cameras and their coexisting software counterparts, allowing autonomous vehicles to be used by the police for crime prevention and detection purposes is a logical and consequential extension of legally permissible uses of technology by the police. Another problem remains however. Even if police use of autonomous vehicles is legally permissible, the use still must successfully pass through the court of public opinion. For example, applying the rationale from Alito's *Jones* concurrence, problems might exist if an autonomous vehicle is used to follow a person for weeks at a time. No physical trespass would occur, but the same information would be gathered as if a GPS monitor was actually attached to a person's property.

B. Social Acceptability of Autonomous Vehicles

When it comes to social acceptability and public perception of police use of autonomous vehicles, there are two distinct issues. The first is the social acceptability of the driverless car itself, and the second is the acceptability and perception of police use of such technology. It is a natural and almost instinctual feeling to have some apprehension of sharing the roads with a car that does not have a person in control of the vehicle. On this possible issue, O. Kevin Vincent, chief counsel of the National Highway Traffic Safety Administration acknowledged in an interview "it is a scary concept for the public," noting that the public is fully aware of what happens when vehicles collide on the road.[53]

[53] John Markoff, *Collision in the Making Between Self-Driving Cars and How the World Works,* N.Y. TIMES (Jan. 23, 2012), http://www.nytimes.com/2012/01/24/technology/googles-autonomous-vehicles-draw-skepticism-at-legal-symposium.html?_r=0.

The biggest concern that the general public will have is how the police use of autonomous vehicles will coexist with their privacy rights and preferences. Public trust and confidence has quickly faded as more revelations come out about the National Security Agency ("NSA") use of technological data, and the technology industry's acquiescence to government demands.[54] The government will have to be completely transparent and open with both the types and amount of information that autonomous vehicles will gather, since they will likely be capable of seeing, hearing, and recording everything around them.

Another concern that the government will have to overcome is the public's notion of "fair play" concerning the law and traffic stops. The public might be reluctant to give up their preference for "human enforcement" of laws.[55] As it stands today, drivers always stand a chance to get away with speeding, illegal U-turns, or running red lights or stop signs because police may exercise discretion in giving out citations based on traffic conditions, locations, and time of day.[56] This arises out of a public view that there is a meaningful distinction between technical legal violations and abiding by the purpose for which the laws exist.[57] If we take the human element out of law enforcement, and an autonomous vehicle automatically records a vehicle speeding, running a stoplight or stop sign, or making an illegal U-Turn, it takes away all discretion, and the general arguments of pretextual stops would be greatly weakened. Many people might run stoplights if stopping appears unwarranted based on the circumstances, like if it

[54] Jackie Calmes & Nick Wingfield, *Tech Leaders and Obama Find Shared Problem: Public Trust,* N.Y. TIMES (Dec. 17 2013), http://www.nytimes.com/2013/12/18/us/politics/as-tech-industry-leaders-meet-with-obama-nsa-ruling-looms-large.html.

[55] Ronald V. Clarke, *Situational Crime Prevention*, 19 CRIME & JUST. 91, 135 (1995).

[56] *Id.*

[57] Joh, *supra* note 48, at 231.

is in a remote location, late at night, with little to no traffic.[58] However, there are two sides to that coin, which will be discussed further in Part III. The same discretion used t o not give a driver a ticket may also be used to pull a driver over based on prejudicial bias.

Perhaps the best way to evaluate the needs for safety and order with society, as well as individual autonomy and privacy rights is to conduct a balancing test. Balancing the opinions that mass surveillance is necessary in deterring crimes and apprehending criminals against the opinions that express privacy and autonomy concerns. Privacy norms center on the unique dignity of each individual human person.[59] In terms of autonomous vehicles and privacy, there are three types of privacy interests that come into play: personal autonomy, personal information, and surveillance.[60] When the vehicle is used for governmental purposes, all three interests become exponentially important. These privacy interests articulate important political considerations regarding the impact these vehicles will have on civil liberties and individual freedoms.[61] All three of these privacy interests play important roles in a well-functioning civil society.[62] These privacy interests will likely be the center of debate, due to the ability for an autonomous vehicle to record an endless amount of video and potentially audio that it picks up as it patrols the streets. This might automatically implicate the privacy rights of individuals who may not want their personal business recorded. In a basic sense, simply collecting massive amounts of data on drivers or civilians on the streets infringes on autonomy, the ability to make

[58] *Id.*

[59] Dorothy J. Glancy, *Privacy in Autonomous Vehicles*, 52 SANTA CLARA L. REV. 1171, 1172 (2012).

[60] *Id.* at 1187.

[61] *Id.*

[62] *Id.*

decisions, and to retain a sphere of private activity free from surveillance.[63] This is not a new concern, as similar objections were made when photo radar first became available.[64] As battles over further privacy rights rage on in the wake of an increasing amount of surveillance, potential use of autonomous vehicles as tools for comprehensively tracking people will affect privacy interests associated with concerns about surveillance.[65] When these vehicles become a viable option for the government as well as the people, these types of privacy interests will have to exist as the cornerstone of regulation and legislation in order to convince and ensure the public that the right of an individual to retain some privacy and autonomy will not be impeded on by autonomous police vehicles. It will likely take entities within industry, academia, and the government working together to establish fair, proper, and legal autonomous vehicle policies.[66]

With the recent public outcry for stronger privacy protections in the wake of NSA revelations, it looks to be an uphill battle for the government to persuade the public that using autonomous vehicles is a good thing, and that they will not amount to any impermissible intrusions on privacy. Two of the strongest arguments the government can use to convince the public to trust the use of these *Knight Rider-RoboCop* hybrids are that they will decrease the amount of discriminatory traffic stops, take subjectivity and discretion out of certain aspects of policing that do not require either, and that they will increase officer safety and police efficiency. The capability of autonomous vehicles to do all of those things will not only help regain public

[63] *Id.*

[64] Some state legislatures responded by banning photo radar use altogether. Survey evidence now shows strong public support for red-light cameras. Robert Puentes, *An Intelligent Transportation Policy*, THE BROOKINGS REV. (2001), *available at* http://www.brookings.edu/research/articles/2001/12/winter transportation-puentes (reporting results of survey by Insurance Research Council that "83% of respondents favor use of red light cameras").

[65] Glancy, *supra* note 59, at 1172.

[66] Dr. Sven A. Beiker, *Legal Aspects of Autonomous Driving*, 52 SANTA CLARA L. REV. 1145, 1153 (2012).

trust in the government and police departments, but will also potentially save valuable taxpayer dollars. These arguments are evaluated in Part III, discussed below.

III. POLICE USE OF AUTONOMOUS VEHICLES WILL BE BENEFICIAL TO SOCIETY

A. Autonomous Vehicles Will Reduce Discriminatory Stops and the Need for Discretion, Decreasing the Amount of Officer Subjectivity

When autonomous vehicles roll onto the streets of the United States in the not-so-distant future, they have the capability to achieve what a seemingly endless amount of regulation and legislation has not yet achieved: the ability to eliminate police discretion from traffic stops.[67] This particular capability has great possibilities and could eliminate prejudicial stops based on race or religion, and could be a significant building block in restoring public trust in police departments and government that has faded tremendously.[68] This has the potential to ultimately lead to safer streets, happier citizens, and a better relationship between the police and the people.

Currently, the use of police discretion in deciding whom they should pursue for potential legal violations can depend on any bias or prejudice that a police officer may have. Legal challenges to police discretion have been made impracticable, if not impossible. Courts give great weight and deference to the discretion of officers, and have allowed simple traffic violations to be considered "reasonable suspicion" for Fourth Amendment purposes.

For example, in *Whren v. United States*, a plainclothes vice officer stopped two African-Americans in a "high drug area" of Washington, D.C. for failing to use a turn signal and driving at an "unreasonable speed."[69] These seemingly minor infractions led to a search of the vehicle,

---

[67] Joh, *supra* note 48, at 199.

[68] *Id.*

[69] *See* Whren v. United States, 517 U.S. 806 (1996).

ultimately resulting in drug charges for the defendants.[70] At trial, the defendants argued that the officer's decision to stop them should have been based on whether a "reasonable officer" would have stopped them.[71]

However, the court disagreed, and found that the stop was reasonable under the Fourth Amendment as long as there was any ground for stopping the defendants, despite the fact that it was against department policy for plainclothes officers to conduct traffic stops.[72] The court reasoned that as long as legal justification existed, the officer's subjective intent was irrelevant.[73] This decision effectively eliminated challenges to evidence obtained by traffic strops for unrelated crimes when police discretion was used as grounds for the stop.[74]

Another failed challenge to an almost glaringly obvious pretextual stop occurred in Texas when the defendant was arrested for failing to wear a seat belt.[75] There, the defendant claimed that even though Texas law permitted the arrest for anyone who failed to wear a seat belt, she was arrested based on the arresting officer's personal animosity towards her.[76] The facts of the case suggest that when the defendant was pulled over, the officer yelled something to the effect of "we've met before," and "you're going to jail."[77] The court rejected defendant's challenge, and reasoned that so long as an officer has probable cause for the offense, an otherwise

---

[70] *Id.* at 806.

[71] *Id.*

[72] *Id.*

[73] *Id.*

[74] Joh, *supra* note 48, at 213.

[75] *See* Atwater v. City of Lago Vista, 532 U.S. 318 (2000).

[76] *Id.* at 324.

[77] *Id.*

permissible warrantless arrest is constitutional.[78] The gravity of this decision was not lost on Justice O'Connor, who noted that there is a potential for abuse in such "unbounded discretion."[79]

As an increasing amount of similar prejudicial stops have come to light, communities – specifically minority communities – have turned to politics to attempt to change the police practice in traffic stops.[80] As a result of state legislation, voluntary departmental changes, and litigation, departments across the nation have begun to collect data on race and ethnicity of motorists in routine traffic stops.[81] Political pressure and media scrutiny have also prompted some police organizations to set forth formal rejections of the use of race as a primary justification for traffic stops.[82] The federal government has followed suit, and issued formal guidelines prohibiting the use of race by federal law enforcement agencies in "traditional law enforcement activities."[83] Racial profiling is so prevalent that the majority of Americans are not only familiar with the practice, but also disapprove of its use.[84] Much like many other political issues, little has been done outside of data collection and formal rejections and renouncements. Despite the widespread attention to these problems, reports of alleged abuses of police discretion remain prevalent.[85]

---

[78] *Id.* at 354.

[79] *Id.* at 372.

[80] Brandon Garrett, *Remedying Racial Profiling*, 33 COLUM. HUM. RTS. L. REV. 41, 82 (2001).

[81] *Id.* at 61-81.

[82] Joh, *supra* note 48, at 215.

[83] Guidance Regarding the Use of Race by Federal Law Enforcement Agencies, U.S. DEP'T OF JUSTICE (2003), *available at* http://www.usdoj.gov/crt/split/documentsguidance_on _race.htm (last visited Feb. 14, 2014).

[84] Garrine P. Laney, *Racial Profiling: Issues and Federal Legislative Proposals and Options*, Cong. Res. Serv. Report RL32231 (Feb 17, 2004), at 5.

[85] Joh, *supra* note 48, at 215.

At first thought, it might be difficult to understand where autonomous vehicles come into play, and how they would have any impact on this issue that has been around for decades. However, if autonomous vehicles were connected with the Intelligent Transport Systems initiative as discussed above, the answer may seem a bit more clear.[86] An automated enforcement program could eliminate stops based on routine traffic stops, like excessive speeding.[87] In order of frequency, the reasons most often cited by the police for traffic stops include speeding, record checks, vehicle defects, stoplight violation, illegal turns, seat belt violations, and suspected drunk driving.[88] Aside from seatbelt violations, all of these reasons would be candidates for automatic enforcement, and could be enforced without the discretion of police officers. These programs would only have a significant impact on eliminating police discretion if the traffic stops are almost 100% automated.[89] This is where autonomous vehicles would have the greatest potential impact.

By driving on its own, the vehicle (and computer inside) does not know the driver's race nor does it harbor any animosity. There is always the potential for discrimination, like if the vehicles are programmed to only minority communities. But the vehicles themselves have no prejudices, and would not be driving down certain streets or neighborhoods just because they are known for being a minority area. By allowing autonomous police vehicles to automatically patrol the streets and detect violations or safety issues, police departments would have substantially limited the amounts of traffic stops conducted by its own officers, eliminating human discretion,

[86] *Id*. at 200.

[87] *Id.* at 221.

[88] *See* MATTHEW R. DUROSE ET AL., U.S. DEP'T OF JUSTICE, CONTACTS BETWEEN POLICE AND THE PUBLIC: FINDINGS FROM THE 2002 NATIONAL SURVEY, iv (2005).

[89] Joh, *supra* note 48, at 222.

potential racial bias, or personal animosity.[90] Not all discretion would be eliminated. Human patrols would still be out on the streets to look for things that autonomous vehicles may not be able to pick up on, as well as give the public an appearance of a safe neighborhood. Autonomous patrols should be meant to supplement, not completely replace humans, and officers or a dispatch would still be able to look in at vehicle's recordings and take calls.

These vehicles would patrol the streets, and would use the technological devices inside the car as well as its connection to the Intelligent Transport System to detect violations. Citations, or even warnings for first time violators, could automatically be mailed to the driver's residence, similar to stoplight or speed cameras, and the driver could challenge the citation using the existing procedures.[91] By implementing an automated system with mailed out warnings, the relationship with the public might increase, and violators would no longer be able blame a perceived quota that must be met as the bases for being stopped for speeding or running a stoplight. An autonomous police car could also help make driving safer, and could become aware of car accidents or malfunctioning cars much more quickly than human officers could. By using its connection to the Intelligent Transport System, the vehicle could pick up "distress signals" from broken down cars, and could respond appropriately. No longer would the *Whren's*[92] or *Atwater's*[93] of the country have a challenge to a conviction based on discretion, racism, or prejudice. While similar defendants would still have broken the law and would have to be held responsible for their actions, these technological innovations significantly reduce the risk of

[90] *Id.* at 223.

[91] *See* Steven Tajoya Naumchik, *Stop! Photographic Enforcement of Red Lights*, 30 MCGEORGE L. REV. 833, 846-47 (1999).

[92] *See generally* Whren and Brown v. United States, 517 U.S. 806 (1996).

[93] *See generally* Atwater v. City of Lago Vista, 532 U.S. 318 (2000).

police discrimination and humiliation. This not only takes some negative connotations away from the police, but also could increase judicial efficiency.

Technological innovations like autonomous vehicles and their use in patrolling the streets could possibly prevent pretextual, discriminatory traffic stops by taking discretion or bias almost entirely out of the picture. This could aid in instilling a new, positive relationship with the public, improve the general reputation of the police force, and prevent humiliating and unnecessary traffic stops. However, the benefits of using autonomous vehicles for police purposes do not stop there. Using these self-driving and semi-self patrolling vehicles creates the potential for increasing the safety of police officers, and they just might be able to increase the efficiency of police departments nationwide.

B. Autonomous Vehicles Will Make Officers Safer and Increase Police Efficiency

By implementing autonomous vehicles into every day use by police departments, the potential is created for an increase in officer safety, and a more efficient, less costly police force. Autonomous police vehicles give police departments around the country the ability to put fewer officers in cars, keeping them out of harms way. Efficiency may also be increased, because these cars allow officers to tend to other crimes, which could possibly be a better use of taxpayer funds. In addition to using taxpayer money more efficiently, they might also be able to reduce the amount police departments rely on, because some police functions could be successfully outsourced to third-party American individuals or groups.

1. Looking at Efficient Models in Other Countries

One of the best ways to model a new system and to foresee how effective it will be is to look at other countries across the world. For purposes of this note, Great Britain will be the most influential and helpful country. Even though most here in America might think that "Big Brother" is most existent in America, Great Britain actually retains the crown for being the "champion of closed-circuit television ("CCTV") surveillance."[94] The British government has access to between two and three million cameras, enabling them to create more video images per capita than any other country in the world.[95] It is not the vast amount of cameras that is important here. What is important is what they actually do with all of that camera footage. Since that amount of footage would be nearly impossible for any governmental agency to sift through and look for potential crimes, Britain's government offers cash rewards to citizens that watch the live-streaming CCTV footage on their home computers and assist the police in apprehending criminals.[96] This is an extremely interesting program, one that has the potential to have great success if implemented in concert with autonomous police vehicles.

Autonomous police vehicles would have cameras equipped on them capable of recording 24 hours a day, seven days a week. Instead of paying an outrageous amount of taxpayer money to workers that would try to sift through the infinite amount of footage, the U.S. government could offer rewards or even tax credits to those who watch the live-streamed footage and assist the police in detecting crime, very similar to what is being done in Great Britain.[97] Surely, some

[94] Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity,* 72 MISS. L.J. 213, 220 (2002).

[95] *Id*. at 220 – 21.

[96] *Internet Eyes, Fighting Crime from Home,* ONTHEMEDIA.ORG, http://www.onthemedia.org/story/ 132939-internet-eyes-fighting-crime-from-home/ (last visited Feb. 13, 2014).

sort of training-type program would be implemented to keep these people from assuming everything they see as a crime, but this could have a tremendous impact on police departments. This would not only save them money, as they have essentially "outsourced" the footage to an outside party, but would also give the public a chance to see what the police see. This, along with giving the public the ability to contribute to the well-being and safety of their area, could go a long way in establishing a healthy, trustworthy relationship with the police, instead of the apprehensive, fearful feelings a lot of the public harbor towards police departments. This truly would be an extension of the "see something, say something" campaign launched by the Department of Homeland Security.[98]

2. Autonomous Vehicles Might Loosen Tight Budgets

Being able to show that autonomous vehicles would be able to help balance budgets and save the police department, and ultimately the government, money could go a long way in determining whether or not they could be used for police purposes. In a time of economic downturn, where between 12,000 and 15,000 police officers have been laid off and a significant amount of officers have been furloughed, money is getting harder and harder to come by for many police departments across the country.[99] This is particularly worrisome, because a reduction in the amount of working police officers can have a direct correlation with an increase

[97] *See* Capers, *supra* note 42, at 963.

[98] *If You See Something, Say Something*, DEP'T OF HOMELAND SECURITY, *available at* http://www.dhs.gov/if-you-see-something-say-something (last visited Feb. 10, 2014).

[99] *The Impact of the Economic Downturn on American Police Agencies*, COMM. ORIENTED POLICING SERVICES, U.S. DEP'T OF JUSTICE (Oct. 2011), http://www.cops.usdoj.gov/files/RIC/Publications/e101113406_Economic%20Impact.pdf (last visited Feb. 10, 2014).

in crime.[100] While the upfront cost of an autonomous vehicle fully equipped with all of the latest technology might be significant, it has the potential to do the work of multiple officers, all while still effectively patrolling neighborhoods.[101] Autonomous police vehicles would become a strong investment, with dividends paying off both financially, as well as in the real world on the streets. Autonomous vehicles could ease the burden that budget cuts and sequestration has caused, and could allow police departments to get back to doing their job, instead of constantly worrying about cutting costs (and corners).

3. Officers Will be Safer With Autonomous Vehicles

Along with efficiency, officer safety is also an ever-growing concern. According to the FBI Uniform Crime Report for 2005, 57,546 police officers were assaulted, with 15,763 resulting in injuries.[102] Over the past decade, on-duty car accidents were responsible for over 450 officer deaths, and a countless amount of injuries.[103] While getting injured or possible even killed is an inherent risk in becoming a police officer, many departments are embracing safety as a core value.[104] Getting hurt is no longer part of the job, and many departments require their officers to

[100] Erica Goode, *After Deep Police Cuts, Sacramento Sees Rise in Crime,* N.Y. TIMES (Nov. 3, 2012), http://www.nytimes.com/2012/11/04/us/after-deep-police-cuts-sacramento-sees-rise-in-crime.html?_r=0.

[101] The cost could very well be over $100,000. Currently, the 3-D sensors in Google's autonomous vehicle alone come in at around $70,000. Brad Plumer, *Here's What It Would Take for Self-Driving Cars to Catch On*, WASH. POST (Oct. 23, 2013), http://www.washingtonpost.com/blogs/wonkblog/wp/2013/10/ 23/heres-what-it-would-take-for-self-driving-cars-to-catch-on/.

[102] Lila Stansups, *How Often Do the Police Get Killed?*, YAHOO! VOICES (Jun. 12, 2007), http://voices.yahoo.com/how-often-police-killed-384148.html?cat=17.

[103] *Causes of Law Enforcement Deaths*, NAT'L LAW ENFORCEMENT OFFICERS MEMORIAL FUND, http://www.nleomf.org/facts/officer-fatalities-data/causes.html (last updated Dec. 30, 2014).

[104] Mark Whitman, *The Culture of Safety: No One Gets Hurt Today*, THE POLICE CHIEF (Nov. 2005), http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=737&issue_id=112005.

go through safety training programs in an effort to reduce the amount of injuries suffered by officers every year.[105] Introducing autonomous vehicles into everyday police use could be one method of helping these "zero injury cultures" achieve their goal. Simply by taking officers off of everyday routine traffic patrol, autonomous vehicles can prevent officers from being injured or killed in car accidents. While officers may not like the idea of being replaced by a computerized machine, knowing that they are going to work every day with a greatly reduced risk of being hurt or killed on the job will give them tremendous peace of mind.

Within the next 25 years, there will be an ever growing demand and need to create a more efficient and less costly police presence across the United States. Along with efficiency, keeping officers safe and out of harms way will also be a goal that will grow ever more important. When the technology is finally perfected and available, there will be an easy mechanism to achieving both safety and efficiency. Autonomous vehicles, while costly upfront, will increase the safety and efficiency of any police department that employs them on their streets.

CONCLUSION

No one knows just quite how the mass production and police use of autonomous vehicles will affect the future of the criminal justice system. Thus far, the only thing that can be done is mere speculation by looking at the current developing technology of these self-driving vehicles, combined with already existing surveillance technology, Fourth Amendment jurisprudence, and other legal analysis. Even though much of the surveillance technologies that these autonomous vehicles will incorporate already exist and are legal to use by police departments, there will likely be cases that make it all the way to the United States Supreme Court once autonomous

[105] *Id.*

police cars are rolled out onto the streets, and it is here where some concrete determinations are made.

If police departments allow use of autonomous vehicles, officers could use their time more efficiently due to autonomous vehicles taking on the load of traffic patrol. Use of autonomous vehicles would also increase officer safety, because fewer officers on the road would risk injury or death from car accidents, and when officers are needed on a scene, they will be more readily prepared. There will also be a reduction of discriminatory stops, because autonomous vehicles will be capable of giving out automatic citations for traffic violations, leaving out any potential animosity or bias. These vehicles will also result in less officer discretion and subjectivity, and a better vehicle for legally permissible evidence gathering. Cumulatively, this will not only result in safer streets and neighborhoods, but also a renewed instillation of trust in police departments and governments across the country.

Some problems may arise due to the vehicles ability to monitor and track suspects 24/7, and record unwilling individuals who rather be left alone. This note has proposed issues and potential solutions for the pro-autonomous vehicle side of the issue. There is no doubt that ever-emerging technology and autonomous vehicles have the potential to change the legal and justice systems as we know it. When thinking about what the future holds in regards to a self-driving police car, one must not rush to the conclusion that they will be RoboCop-Knight Rider hybrids that are capable of going after crime rings and dangerous criminals. These cars will have to abide by the same laws as non-autonomous vehicles, as well as laws governing evidence collecting and the constitution. As the prototypes and ideas of autonomous vehicles turn into reality, we must be ready to adapt, expand, and understand our laws to maintain their underlying purpose.

SYRACUSE JOURNAL OF SCIENCE & TECHNOLOGY LAW

VOLUME 31 2014-2015 ARTICLE 7, PAGE 184

DOMESTIC PRESENCE IN THE SKIES: WHY AMERICANS SHOULD CARE ABOUT PRIVATE DRONE REGULATION

By: Tyler Hite[1]

ABSTRACT

The concept of an unmanned aerial vehicle has largely been considered one of America's most innovative and advantageous military accomplishments within the past two decades. However this technology, while not armed with Hellfire missiles or powerful high-altitude long endurance capabilities, is rapidly becoming available to private citizens for lower altitude and short range operations. As these drones are also becoming reasonably affordable, federal and state regulations are just now emerging to respond to safety, security, and privacy concerns regarding private drone operation. This paper seeks to provide an overview of what private drones are, the state and federal regulations currently being developed, as well as those already in place, and proposes the implementation of registration and licensing procedures for private drone operation.

[1] Syracuse University College of Law, Juris Doctor expected 2015. I would like to thank Professor William C. Banks for his encouragement and help throughout the development of this note.

INTRODUCTION

Within the past decade, drone strikes and the concept of Unmanned Aerial Vehicles (UAVs) have become not only commonplace among major news headlines, but continue to lead the way for modern warfare tactics and strategy. With precision missile and surveillance capabilities, Predator drones have led to the successful elimination of high-valued targets listed as terrorists by the United States. However such success is not absolute, with several documented mishaps ending with civilian casualties. While the United States Military continues to implement UAVs overseas, American citizens should become cognizant that drone activity above U.S. soil is on the precipice of a market explosion comparable to that of Apple in the 1980's.[2] Yet these drones will not be operated by military personnel under specific military orders, but by fellow citizens, local governmental officials, and even neighbors regulated by yet-to-be developed laws and restrictions.

Thus the driving question becomes, what limitations will be developed for individuals who purchase and operate private drones? With some drones currently on sale for as little as $300, potential problems are primed to become actual issues. Additionally, federalism concerns arise regarding whether the regulation of drones will be left to the States to decide how to craft restrictions within their jurisdiction, or whether the Federal government is better suited to enforce private drone regulations. This paper will attempt to shed light not only on the capabilities and functions of privately owned drones, developed for use by private individuals, but will also look to the developing regulations already emanating from both state and federal governments, and how those regulations will shape the expansion of the private drone market.

[2] Tim Fernholz, *The Private Drone Industry Is Like Apply in 1984*, QUARTZ (Jan. 25, 2013), http://qz.com/46893/the-private-drone-industry-is-like-apple-in-1984/.

While legislators still have yet to determine the exact guidelines for private drone operation, the logical solution seems to be registration and licensing of unmanned aerial vehicle operation, either with the federal government or the several states.

I. PRIVATE DRONES

Unmanned aerial vehicles currently exist under various classifications depending on size and capability. This section will first address how agencies attempt to define and classify what a drone is, and then shift to the actual composition of various drone designs.

A. Classifications

Unmanned aircraft have been known by many names, including "drones, remotely piloted vehicles (RPV), unmanned aerial vehicles (UAV), models, and radio control (R/C) aircraft," but today are generally referred to as unmanned aerial systems (UAS) to encompass various aerial vehicles which are remotely piloted without a pilot.[3] As can be expected, the technology associated with private drones is developing at a rapid and unrelenting pace, with manufacturers implementing already well-developed technology, such as GPS, real-time streaming video connection, and high resolution cameras, to enhance the abilities and sophistication of privately manned aerial vehicles. On the heels of such progress, law-makers are still attempting craft appropriate legislation in response to the many concerns citizens possess regarding privacy and safety with UAS flying above.

[3] *Integration of Civil Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS) Roadmap*, U.S. DEPARTMENT OF TRANSPORTATION: FEDERAL AVIATION ADMINISTRATION, (Nov. 7, 2013), http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CCQQFjAB&url=http%3A%2F%2Fwww.faa.gov%2Fuas%2Fmedia%2Fuas_roadmap_2013.pdf&ei=HV4oVbuHEomGyQTm8oHwCg&usg=AFQjCNG49jblwiI3-APRm6ZmV-xdfKyRpw&sig2=2rFeAtcnKvU2sjIBLoCksw&bvm=bv.90491159,d.aWw&cad=rja.

Within the context of policy development and regulation, the FAA has noted that a primary hindrance to uniform restrictions on Unmanned Aerial Systems is their lack of universal design.[4] Even larger issues arise when attempting to interpret current FAA regulations and determine which regulations apply to a certain UAS.[5] When breaking down any privately available drone, the components and versatility of assembly makes nearly every drone unique, even though components perform the same functions. Depending on the scale of the drone, the exact same setup can lead to extravagant performance differences.

Without consensus on classifications for UAS flight in civil airspace, current definitions are consistent with nomenclature used by research and military communities.[6] Classifications such as micro, mini, tactical, medium altitude and high altitude unmanned combat air vehicles (UCAV) are implemented to refer to UAS depending upon their mission requirements.[7] Most civilian UAS applications which will be available for purchase fall within the micro and small UAS categories, however the large performance ranges and varying capabilities of privately owned drones create classification issues.[8] For instance, Micro UAS are between 1 and 4.5 pounds, less than three feet in size, travel anywhere from 10 to 25 miles per hour, fly at less than 3,000 feet, and possess an endurance of less roughly 1 hour.[9] Small UAS weigh between 4.5 and 55 pounds, are less than 10 feet in size, fly to an altitude of up to 10,000 feet, can travel between

[4] Integration of Civil Unmanned Aircraft Systems, *supra* note 3.

[5] *Id.*

[6] Unmanned Aircraft System (UAS) Service Demand 2015-2035, U.S. AIR FORCE, AEROSPACE MGMT. SYS. DIV., http://ntl.bts.gov/lib/48000/48200/48226/UAS_Service_Demand.pdf.

[7] *Id.*

[8] *Id.*

[9] Unmanned Aircraft System, *supra* note 6, at 117.

50 and 75 miles per hour, and possess and endurance of 1 to 4 hours.[10] The smallest drones, categorized as nano, have severely limited capabilities as they weigh less than 1 pound, are less than 1 foot in size, fly less than 400 feet in altitude, travel at less than 25 miles per hour, and have an endurance of less than 1 hour.[11] But these categorizations are not absolute, as variances in performance output and overall design can place a drone in multiple categories.

B. General Design

Without doubt, the intended application of each drone dictates every aspect of a drone's composition. Beginning with the basics, most private drones are composed of centralized battery operated power system, although some savvy engineering students have successfully developed gas powered drones.[12] This power system is typically mounted near the center of each drone on the drone's frame, and powers a varying number of rotors and propellers mounted around the exterior of the drone's frame, often referred to as quadcopters, hexacopters, or octocopters depending upon the number of propellers used to send the drone into flight.

The frame of drones falls within one of two categories, either fixed-wing or rotary.[13] Fixed-wing structures are comparable to the model airplanes of the past, and imitate small scale versions of commercial airliners, military aircraft, and smaller privately owned aircraft. Rotary drones, on the other hand, resemble the type of automated flying machines fit for the latest box-

---

[10] *Id.*

[11] Unmanned Aircraft System, *supra* note 6, at 117.

[12] "Incredible HLQ (Heavy Lift Quadcopter)", Incredible HLQ Engineering Team, 2014, https://www.kickstarter.com/projects/1671680066/incredible-hlq-heavy-lift-quadcopter?ref=home_location; "Parrot AR. Drone 2.0 Elite Edition," PARROT, http://ardrone2.parrot.com/; "Information on Building your own UAV", Build A Drone, http://www.buildadrone.co.uk/multicopter-drone-components.html

[13] *UAV: Fixed Wing or Rotary?,* SUAS NEWS, (Sept. 24, 2013), http://www.suasnews.com/2013/09/25214/uav-fixed-wing-or-rotary/.

office sci-fi hit. Often resembling the central hub and spokes of a western wagon wheel, these drones utilize the thrust of multiple propellers mounted in a circular fashion around the center of the drone's fuselage. Comparable to the upward thrust of a helicopter, drones are able to use multiple-propellers to travel in all directions and hover.[14]

Pilots of privately operated drones have a multitude of options to control their UAS, from downloadable phone applications which force a drone to respond to the varying tilt angles of the cell phone, to immensely complicated radio transmitters and receivers that command drones to maintain a particular altitude, hover, return to a certain point, or even land at a fixed and convenient location.[15] Autopilot platforms are software driven, thus it is easy to comprehend how the possibilities for what a drone can do on its own is nearly endless at the hands of skilled and creative programmer. Currently available to the public, GPS flight controllers utilize multi-processor systems, inner dampeners, controllers, gyroscopes, accelerometers and barometers to send critical data to a drone's internal computer, which analyzes the data and optimizes flight capabilities.[16]

Beyond the design of a drone, and of primary interest to this paper, is what types of technology and devices and be carried by drones. Amazon recently created a flurry interest regarding their development of automated drone delivery systems, Prime Air, capable of 30

---

[14] *UAV: Fixed Wing or Rotary?*, sUAS NEWS, (Sept. 24, 2013), http://www.suasnews.com/2013/09/25214/uav-fixed-wing-or-rotary/; Glenn Derene, *The Art of Flying Your Very Own Drone*, POPULAR MECHANICS, (Oct. 22, 2013), http://www.popularmechanics.com/technology/aviation/diy-flying/the-art-of-flying-your-very-own-drone-16068825.

[15] *Parrot AR. Drone 2.0 Elite Edition*, PARROT, http://ardrone2.parrot.com/ (last visited Mar. 20, 2015); *Information on Building your own UAV*, BUILD A DRONE, http://www.buildadrone.co.uk/multicopter-drone-components.html (last visited Mar. 20, 2015).

[16] *DJI Naza GPS Flight Controller*, BYOD, http://www.buildyourowndrone.co.uk/DJI-NAZA-GPS-Flight-Controller-p/dji-nazagps.htm (last visited Mar. 20, 2015); Chris Anderson, *A Newbie's Guide to UAVs*, DIY DRONES (Mar. 28, 2009, 2:00 PM), http://diydrones.com/profiles/blogs/a-newbies-guide-to-uavs.

minute delivery of small packages weighing less than 5 pounds.[17] While intriguing, Amazon's Prime Air has been criticized as a public relations stunt more than an actual program development, as obvious obstacles of thievery, weather conditions, payload capabilities and flight time have yet to be addressed directly by Amazon officials.[18] The real concern created by private drones appears once high-definition cameras, recorders, and weapons are attached and flown without proper regulation, restrictions, or due regard for the rights of others.

Wireless video add-ons are currently capable of transmitting real-time video with no interference at a 3 kilometer range, and can be extending to over 14 kilometers with additional transmission equipment.[19] Real-time footage can be sent to small screens mounted directly to drone controllers, or even to specially developed goggles which matches the operator's view with that of the drone.[20] Major companies, including Verizon Wireless, have already began to advertise and prepare for the upcoming drone market explosion, creating cell phone applications which receive real time video footage from drone surveillance cameras, and further allow the user to directly upload their recorded footage to their computers, popular social media websites, or even YouTube.[21]

In addition to surveillance capabilities, some drone owners have not left behind the concept of military-capable drones, and have created trigger mechanisms which operate

---

[17] *Amazon Prime Air*, AMAZON, http://www.amazon.com/b?node=8037720011 (last visited Mar. 20, 2015).

[18] Doug Gross, *Amazon's drone delivery: How would it work?*, CNN TECH (Dec. 2, 2013, 5:57 PM), http://www.cnn.com/2013/12/02/tech/innovation/amazon-drones-questions/.

[19] Robert Krogh, *New 5.8 Ghz wireless video system 1200mW Long Range*, DIY DRONES (Sept. 1, 2012, 12:00 AM), http://diydrones.com/profiles/blogs/new-5-8-ghz-wireless-video-system-1200mw-long-range.

[20] *Wireless Video LCD Goggles Downlink Kit*, STEADIDRONE, http://shop.steadidrone.eu/product/wireless-video-lcd-goggles-downlink-kit/ (last visited Mar. 30, 2015).

[21] Brian Plaskon, *Rediscover the Magic of Flight with the Parrot AR.Drone 2.0*, VERIZON (Dec. 16, 2014), http://www.verizonwireless.com/news/article/2013/12/ar-parrot-drone.html.

handguns and paintball guns attached to the drone.[22] In another widely viewed video, although touted as fake, has raised concerns regarding the possibility of accurate and easily controlled machine guns mounted to drones. While drone manufactures have not advertised for the ability of drone owners to weaponize their drone, the mechanisms needed to arm a drone are nowhere near complicated enough to deter drone owners from attempting to attached smaller pistols and lightweight handguns to the drone. Combined with real-time high-definition video footage, sophisticated programming, agile maneuvering capabilities, and long-range drone applications, it is not beyond comprehension that an armed drone placed in the wrong hands could potentially lead to life-threatening circumstances.

Fortunately one such plot has already been discovered and foiled. Recently captured by FBI agents, Rezwan Ferdaus, an admitted Islamic extremists, hatched a plan to attack the United States Capitol Building and the Pentagon by flying several model aircrafts loaded with C4 explosives into the buildings.[23] Ferdaus's plot envisioned flying small global positioning system (GPS) operated drones from several locations before launching ground assaults in the Capitol.[24] His drone of choice was a fixed wing F-86 sabre model air plane, and while he possessed over 25 pounds of C4 to load onto the plane, model air plane experts were very doubtful that such an attack could be carried out without drawing a significant amount of attention to Ferdaus during

---

[22] *Flying Drone Armed with a Handgun*, MILITARY.COM (June 8, 2013), http://www.military.com/video/guns/pistols/flying-drone-armed-with-handgun/2487684756001/; Evan Ackerman, *Man Puts (Paintball) Gun on Quadrotor But Don't Panic*, IEEE SPECTRUM (Dec. 13, 2012), http://spectrum.ieee.org/automaton/robotics/diy/paintball-gun-on-quadrotor-but-dont-panic.

[23] D.J. Marks, *Massachusetts Man to Plead Guilty in Model Plane Terror Plot,* ABC NEWS (July 10, 2012), http://abcnews.go.com/Blotter/massachusetts-man-plead-guilty-model-plane-terror-plot/story?id=16748584.

[24] Carmen M. Oritz, *Ashland Man Charged with Plotting Attack on Pentago and U.S. Capitol and Attempting to Provide Material Support to Foreign Terrorist Organization*, DEPT. OF JUSTICE (Sept. 18, 2011), http://www.investigativeproject.org/documents/case_docs/1691.pdf.

the attack.[25] Requiring a significant runway and competent pilot, the F-86 sabre model was far from ideal for a calculated attack.[26] Although Ferdaus was captured when trying to purchase the explosives from undercover agents, his plot shows that an attack by a private drone operator is quite possible, and with more developed drones becoming widely available, the likelihood of successful attacks being undertaken continues to increase.

Critics of Ferdaus's attack mocked the lack of plausibility associated with his plan, as take-off and control of this particular model airplane requires a large space of land and a proficient operator.[27] But this unmanned aerial vehicle was modeled after a fighter jet as a fixed wing propulsion vehicle vastly different than the types of drones becoming available for purchase. Instead, these drones incorporate sophisticated software and communication systems which allow for uncomplicated flight operation and control. New UAS are also designed for vertical take-off, and can even be programmed for autonomous flight operations such as taking off, hovering, returning to take-off location, and landing. In fact, one of the most popular drones currently on the market, the Parrot AR 2.0, is capable of phone and iPad interface controls, simple controls capabilities, and fairly sophisticated flight performance.[28] One such operator demonstrated the various capabilities of his Parrot AR 2.0, and it does not take much imagination to visualize the same type of drone spying on others in the near vicinity.[29]

---

[25] Kevin Johnson, *Man Accused of Plotting Drone Attacks on Pentagon, Capital*, USA TODAY (Sept. 29, 2011), http://usatoday30.usatoday.com/news/washington/story/2011-09-28/DC-terrorist-plot-drone/50593792/1; Neal Ungerleider, *The Science Behind the Drone Terrorism Attack*, FAST COMPANY (Sept. 29, 2011, 12:45 AM), http://www.fastcompany.com/1783721/science-behind-drone-terrorism-attack.

[26] Ungerleider, *supra* note 25.

[27] *Model Airplanes a New Terrorist Weapon? Experts Say They Pose Little Threat*, FOXNEWS.COM (Sept. 30, 2011), http://www.foxnews.com/us/2011/09/29/could-model-airplanes-be-next-terrorist-weapon/.

[28] *Linus Tech Tips: Parrot AR Drone iPad Controlled Remote Control Aircraft Test Flight,* YOUTUBE.COM (Aug. 4, 2011), https://www.youtube.com/watch?v=bkKeijmgXW0.

[29] *Id.*

II. CURRENT FEDERAL REGULATIONS

With increase in market availability of unmanned aerial vehicles comes the need for regulation. Recent estimates indicate that by 2035, federal and state sector agencies, including first responders, metropolitan police, and local governments, will possess nearly 36,000 UAS vehicles.[30] The current U.S. market includes over 200 model aircraft manufacturers, with the total number of radio controlled or autonomous flying models exceeding 500,000, with most capable of commercial UAS applications.[31] Clearly the sheer number of potential UAS available for flight in the NAS has pressured the FAA to develop policies capable of managing and overseeing the safe operation of these UAS, though regulations are still in research and development phases of enactment.

The Federal Aviation Administration (FAA) currently asserts authority over the regulation of private drone use, stating that "a key activity of the FAA is to develop regulations, policy, procedures, guidance material, and training requirements to support safe and efficient UAS [unmanned aerial systems] operations in the NAS [National Airspace System], while coordinating with relevant departments and agencies to address related key policy areas of concern such as privacy and national security."[32] The FAA has compiled a list of potential

---

[30] *Unmanned Aircraft System (UAS) Service Demand 2015-2035*, U.S. DEPARTMENT OF TRANSPORTATION, 133 (Sept. 2013), http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&ved=0CCQQFjAA&url=http%3A%2F%2Fntl.bts.gov%2Flib%2F48000%2F48200%2F48226%2FUAS_Service_Demand.pdf&ei=64YCU9-TLa3p0QHIrYDoBw&usg=AFQjCNFG1XuduiEKzrkHDBCaihi4_vhADw&bvm=bv.61535280,d.dmQ

[31] *Id.*

commercial and civilian UAS applications, of which include "security awareness, disaster response (including search and support to rescuers), communications and broadcast (including news/sports event coverage), cargo transport, spectral and thermal analysis, critical infrastructure monitoring (including power facilities, ports, and pipelines), and commercial photography (aerial mapping, charting, and advertising)."[33] While not an exhaustive list, the FAA's consideration of the numerous applications available for drones exemplifies just how versatile this upcoming market has become.

The FAA, in order to assure the safety of the NAS, crafts regulations and policies based upon three areas of concern: (1) equipment; (2) personnel; and (3) operations and procedure.[34] For UAS applications, the FAA summarized four key points from the *FAA Notice of Policy: Unmanned Aircraft Operations in the National Airspace System*, which must be met in order for limited operations to be undertaken by UAS pilots.[35] Each point is aimed at ensuring the safety of the general public, other UAS users, and manned airplanes being flown within the NAS.[36] Specifically,

> [1] regulatory standards need to be developed to enable current technology for unmanned aircraft to comply with Title 14 Code of Federal Regulations; [2] In order to ensure safety, the operator is required to establish the UAS airworthiness either from FAA certification, a Department of Defense (DOD) airworthiness statement, or by other approved means; [3] Applicants also have to demonstrate that a collision with another aircraft or other airspace user is extremely improbable; [4] And the pilot-in-command concept is essential to the safe operation of manned operations – the FAA's UAS guidance applies this pilot-in-

[32] Integration of Civil Unmanned Aircraft Systems, *supra* note 3.
[33] *Id.*

[34] Integration of Civil Unmanned Aircraft Systems, *supra* note 3.

[35] Unmanned Aircraft Operations in the National Airspace System, 72 Fed. Reg. 6689 (proposed Feb. 13, 2007) (to be codified at 14 C.F.R. pt. 91).

[36] Integration of Civil Unmanned Aircraft Systems, *supra* note 3.

> command concept to unmanned aircraft and includes minimum qualification and currency requirements.[37]

The FAA is also influenced by RTCA, Inc., a private not-for-profit corporation that collects information regarding communications, navigation, surveillance, and air traffic management system issues.[38] Within the context of UAS integration into the NAS, the RTCA recommended 8 requirements summarized by the FAA as follows: "[1] UAS must operate safely, efficiently, and compatibly with service providers and other users of the NAS so that overall safety is not degraded; [2] UAS will have access to the NAS, provided they have appropriate equipage and the ability to meet the requirements for flying in various classes of airspace; [3] Routine UAS operations will not require the creation of new special use of airspace, or modification of existing special use airspace; [4] Except for some special cases, such as small UAS (sUAS) with very limited operational range, all UAS will require design and airworthiness certification to fly civil operations in the NAS; [5] UAS pilots will require certification, though some of the requirements may differ from manned aviation; [6] UAS will comply with ATC instructions, clearances, and procedures when receiving air traffic services; [7] UAS pilots (the pilot-in-command) will always have responsibility for the unmanned aircraft while it is operating; [8] UAS commercial operations will need to apply the operational control concept as appropriate for the type of operation, but with different functions applicable to UAS operations."[39]

Currently, UAS operations are not authorized in Class B airspace, which exists over major urban areas containing "the highest density of manned aircraft in the National Airspace

---

[37] *Id.*
[38] *Id.* at 11.

[39] Integration of Civil Unmanned Aircraft Systems, *supra* note 3.

System."[40] To gain approval from the FAA to operate a UAS, an operator must either obtain an experimental airworthiness certificate for private sector aircraft to do research and development, training, and flight demonstrations; or must obtain a Certificate of Waiver or Authorization for public aircraft.[41]

However, Class B prohibitions still apply to UAS.[42] Public entities who request and receive a Certificate of Waiver or an Authorization for uses such as law enforcement, firefighting, border patrol, disaster relief, search and rescue, military training, and other government operational missions, are then allowed to operate UASs in a defined block of airspace with restrictions specific to the unique use of the UAS within that zone.[43] The most notable restriction placed upon operators is the requirement that the operator coordinate with an appropriate air traffic control facility; a restriction which can severely increase the costs of UAS operations and limit the use of UASs in emergency situations. Since 2009, the issuance of Certificates of Waiver or Authorization has more than tripled, from 146 to 545 as of December 4, 2013.[44]

As for privately operated UASs, the FAA Advisory Circular 91-57 establishes the requisite operating standards for UAS pilots-in-command.[45] Aimed at avoiding hazard, the

---

[40] *Fact Sheet – Unmanned Aircraft Systems (UAS)*, FED. AVIATION ADMIN. (Jan. 6, 2014), http://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=14153.

[41] *Id.*

[42] *Id.*

[43] Fact Sheet – Unmanned Aircraft Systems, *supra* note 40.

[44] *Id.*

[45] *Id.*; Advisory Circular, June 9, 1981, DEPARTMENT OF TRANSPORTATION: FEDERAL AVIATION ADMINISTRATION, http://www.faa.gov/documentLibrary/media/Advisory_Circular/91-57.pdf.

Advisory Circular is also meant to "create a good neighbor environment with affected communities and airspace users."[46] The circular mandates operators

> [1] select and operating site that is of sufficient distance from populated areas. The selected site should be away from noise sensitive areas such as parks, schools, hospitals, churches, etc.; [2] Do not operate model aircraft in the presence of spectators until the aircraft is successfully flight tested and proven airworthy; [3] Do not fly model aircraft higher than 400 feet above the surface. When flying aircraft within 3 miles of an airport, notify the airport operator, or when an air traffic facility is located at the airport, notify the control tower, or flight service station; [4] give right of way to, and avoid flying in the proximity of, full-scale aircraft. Use observers to help if possible; [5] do not hesitate to ask for assistance from any airport traffic control tower or flight service station concerning compliance with these standards.[47]

The most obvious logistical obstacle for policy development is how to accurately respond to UAS systems operating in the NAS with varied and potentially unreliable performance capabilities. Without a pilot in an aircraft, or without proper communications equipment, navigation and awareness of other airplanes is greatly diminished.[48] The ability for smaller UAS to change flight patterns or adhere to current operational rules has not been well researched, requiring the FAA to open 6 test site facilities around the country to collect data and better understand how the integration of UAS into the NAS will occur.[49] These operators were meant to achieve "cross-country geographic and climatic diversity and help the FAA meet its UAS research needs."[50] These facilities include the University of Alaska (developing a set of standards for unmanned aircraft categories, state monitoring, and navigation), the State of Nevada

---

[46] Advisory Circular, June 9, 1981, DEPARTMENT OF TRANSPORTATION: FEDERAL AVIATION ADMINISTRATION, http://www.faa.gov/documentLibrary/media/Advisory_Circular/91-57.pdf.
[47] *Id.*

[48] Integration of Civil Unmanned Aircraft Systems, *supra* note 3.

[49] *Id.*

[50] Fact Sheet – Unmanned Aircraft Systems, *supra* note 40.

(concentrating on UAS standards and operations as well as operator standards and certification requirements), New York's Griffiss International Airport (developing test and evaluation processes, along with verification and validation processes under FAA safety oversight), the North Dakota Department of Commerce (developing airworthiness essential data and validating high reliability link technology), Texas A&M University in Corpus Christi (developing system safety requirements for UAS vehicles and operations with a goal of protocols and procedures for airworthiness testing), and the Virginia Polytechnic Institute and State University (Virginia Tech – conducting UAS failure mode testing and identifying and evaluating operational and technical risk areas).

A recent FAA Reauthorization Bill further directed the FAA to restrict government public safety agency's operation of unmanned aircraft weighing 4.4 or less.[51] Specifically, these UAS "must be flown within the line of sight of the operator, less than 400 feet above the ground, during daylight conditions, inside Glass G (uncontrolled) airspace and more than 5 miles from any airport or other location with aviation activities."[52] But this regulation is limited only to public use of drones, not private use. In fact, the FAA has only promulgated guidelines for operating drones under certain conditions, but has yet to enact restrictions on what operators are not allowed to do with their drone, such as flying over other individual's property or home while recording video or taking pictures. Under these guidelines, perhaps an aggrieved party can rely upon other privacy oriented laws within their state to seek injunctive relief from such flights, or even damages if warranted, but the potential for privacy violations seems clearly severe enough to warrant direct and explicit legal prohibitions.

[51] FAA Modernization and Reform Act of 2012, Pub. L. No. 112-95, § 334(c) (2012); Fact Sheet – Unmanned Aircraft Systems, *supra* note 40.

[52] Fact Sheet – Unmanned Aircraft Systems, *supra* note 40.

III. STATE REGULATION

Since the FAA is charged with "ensuring the safe and efficient use of U.S. airspace," most state laws and regulations are effectively pre-empted if they concern airspace regulation.[53] States still have the power and authority to regulate use of UAS by public officials and government entities, yet restrictions on private individual's use of UAS falls under the authority of the FAA.[54] Regardless, in 2013 43 states introduced 130 bills and resolutions addressing UAS issues, leading to 13 states enacting 16 new laws and 11 states adopting 16 resolutions.[55] The following ten state laws and proposed legislation exhibits the emerging and evolving nature of drone regulation across the nation. In general, states have similar ideas on the current need of enacted legislation to respond to concerns regarding drones, but most state laws limit their regulation to that of state agencies.

A. Florida

Florida's recent law, titled the Freedom from Unwarranted Surveillance Act, specifically targets the use of drones by law enforcement entities.[56] The law prohibits any law enforcement agency from collecting evidence by means of drone technology.[57] The law carries one exception, whereby a police agency may implement drones to "counter a high risk of a terrorist attack by a

---

[53] *Id.*
[54] *Id.*

[55] *2013 Unmanned Aircraft Systems (UAS) Legislation*, NCSL (2014), http://www.ncsl.org/research/civil-and-criminal-justice/unmanned-aerial-vehicles.aspx.

[56] Joe Sutton & Catherine E. Shoichet, *Florida Gov. Rick Scott signs Law restricting drones*, CNN U.S. (Apr. 28, 2013, 1:42 PM), http://www.cnn.com/2013/04/25/us/florida-drone-law/; S.B. 92, 2013 Leg., Reg. Sess. (Fl. 2013).

[57] S.B. 92, 2013 Leg., Reg. Sess. (Fl. 2013).

specific individual or organization if the United States Secretary of Homeland Security determines that credible intelligence indicates that there is such a risk."[58] If violated, the aggrieved party is entitled to bring a civil action for relief to prevent or remedy such violations.[59] But this action extends only to law enforcement agencies collecting evidence by means of drone technology, not that of private individuals.

Aggrieved parties are entitled to file a civil action in order to "prevent or remedy a violation of this act."[60] All evidence obtained in violation of this section is not admissible as evidence in a criminal prosecution within the state, but the law fails to consider or address the use of evidence in a civil action.[61] Thus if an individual, not a law enforcement agency, gathers information or evidence with the use of a drone, Florida's law takes no steps to exclude such evidence in a civil matter.

B. Hawaii

Hawaii's legislature, recognizing "its duty to protect Hawaii residents from threats to their constitutional rights to privacy," introduced Senate Bill 2608 earlier this year which targets the use of unmanned aircraft technology.[62] This bill seeks to amend the Hawaii Revised Statutes by strictly prohibiting the gathering of information including, but not limited to images, photographs and recordings by unmanned aircraft.[63] Prohibitions extend to law enforcement agencies, state or

---

[58] *Id.*

[59] *Id.*

[60] *Id.*

[61] S.B. 92, 2013 Leg., Reg. Sess. (Fl. 2013).

[62] S. 2608, 27 Leg., Reg. Sess. (Haw. 2014).

[63] *Id.*

local public agencies, persons, and entities.[64] Therefore any operator of a UAS in the state of Hawaii is bound to the regulations Senate Bill 2608 imposes.

803-C allows for five exceptions to the general prohibitions, granting the use of drones in limited circumstances by law enforcement agencies.[65] These exceptions include the receipt of credible intelligence by the United States Secretary of Homeland Security that the use of unmanned aircraft is required to counter a terrorist attack, by issuance of a search warrant not exceeding 30 days, use of unmanned aircraft necessary to assist in search and rescue activities, use by any branch of the military, or if unmanned aircraft needed to assist with disaster relief.[66] Aggrieved parties may seek a remedy, including actual and general damages, attorney's fees, and other damages in an amount no less than $1,000. Further, if information collected by an unmanned aircraft was publicly disclosed without an aggrieved party's permission, then they can collect the same damages in an amount no less than $10,000.[67]

C. Idaho

Senate Bill 1067 focused on restricting drone surveillance by persons, entities and state agencies for the purpose of gathering evidence pertaining to criminal conduct or violations of Idaho's law unless explicitly authorized to do so by an issued warrant.[68] When unconnected to gathering evidence relating to a violation of law, the bill further prohibited surveillance of any individual, property owned by an individual, farm or agricultural industry without the consent of

---

[64] *Id.* at 803-B.
[65] *Id.* at 803-C.

[66] *Id.*

[67] S.B. 2608, 27 Leg., Reg. Sess. §803-F (Haw. 2014).

[68] S.B. 1067, 62nd Leg., 1st Sess. (Idaho 2013).

that individual.[69] However, if an individual owns a facility on the land of another, they are not restricted from implementing a UAS to inspect the facility.[70] Exceptions are incorporated to allow law enforcement agencies to use unmanned aircraft if an exigent circumstance exists, defined as a law enforcement agency possessing "reasonable suspicion that, under particular circumstances, swift action to prevent imminent danger to life is necessary."[71] Remedies allow aggrieved parties to collect all appropriate relief, and no evidence obtained by an unmanned aircraft without a valid warrant is admissible in a court of law.[72]

Additionally, SB 1134, which was signed into law April 11, 2013, more broadly address civilian UAS by defining unmanned aircraft systems as "unmanned aircraft vehicle, drone, remotely piloted vehicle, remotely piloted aircraft or remotely operated aircraft that is a powered aerial vehicle that does not carry a human operator," but not including "model flying airplanes or rockets."[73] The restrictions under this law carry the prohibition of the use of unmanned aircraft systems for surveillance purposes unless by warrant, except in situations where such surveillance is used for emergency response for safety, search and rescues, or controlled substance investigation.[74] The law further specifies that surveillance of individuals and their property, such as their property's curtilage, is prohibited without written consent of the owner.[75] Aggrieved

---

[69] *Id.* at § 3 (2).
[70] *Id.*

[71] *Id.* at § 4 (21-215).

[72] *Id.* § 5 (2).

[73] S.B. 1134, 2013 Leg., 1st Sess. (Idaho 2013).

[74] *Id.*

[75] *Id.*

individuals are entitled to file a civil action for any violation of this law for the greater of $1,000 or actual and general damages including reasonable attorney's fees.[76]

D. Illinois

Illinois has recently enacted two laws targeting the use and operation of drones within the state. The first, HR 1652, was established in response to actions by People for the Ethical Treatment of Animals (PETA). PETA announced plans to use privately controlled drones to spy on and interfere with hunters in the state in an attempt to gather evidence of hunters engaged in illegal activities.[77] HR 1652 amends Illinois' Fish and Aquatic Life Code by making it a misdemeanor for anyone who "uses a drone in a way that interferes with another person's lawful taking of wildlife or aquatic life."[78] Compared to other states, this is one of the most active stances against the use of privately controlled UAS, and may indicate Illinois' willingness to restrict the use of drones when that use infringes upon the rights of others.

Additionally, SB 1587 prohibits the use of drones by law enforcement agencies in all situations except five.[79] These five exceptions include countering a high risk of a terrorist attack, after obtaining a search warrant based upon probable cause, when swift action is needed to prevent imminent harm to life or to forestall the imminent escape of a suspect of the destruction of evidence, when the agency is attempting to locate a missing person, and solely for the

---

[76] *Id.*

[77] Chistopher Zara, *PETA Hunter Drones Shot Down By Illinois Law? 'Air Angels' Will Still Fly, Says Animal-Rights Group*, INT'L BUS. TIMES, Jan. 03, 2014, http://www.ibtimes.com/peta-hunter-drones-shot-down-illinois-law-air-angels-will-still-fly-says-animal-rights-group-1525978.

[78] Illinois General Assembly, Public Act 098-0402, http://ilga.gov/legislation/publicacts/fulltext.asp?Name=098-0402

[79] Illinois General Assembly, Public Act 098-0569, http://ilga.gov/legislation/publicacts/fulltext.asp?Name=098-0569.

purposes of crime scene and traffic crash scene photography.[80] Legislators also saw fit to allow information that is obtained under these exceptions to be retained for longer than 30 days if there is "(1) reasonable suspicion that the information contains evidence of criminal activity; or (2) the information is relevant to an ongoing investigation or pending criminal trial."[81] This information may be disclosed to another government agency, and can be admitted into evidence if the information is found to fall under a "judicially recognized exception to the exclusionary rule of the 4th Amendment of the U.S. Constitution or Article I, Section 6 of the Illinois Constitution."[82]

E. Maryland

Legislators in Maryland began 2014 by introducing multiple pieces of legislation restricting the ability of law enforcement to use and implement drones for surveillance purposes, with one legislator stating "drones shouldn't be flying over our homes, spying on us in our backyard."[83] To this effect, Maryland's recent legislation is proposing one of the most detailed and comprehensive laws restricting the use of drones. HB 847 and SB 926 first approach the definition of "drone" in a different manner than other states by focusing on the level of immediate control an individual has over the vehicle rather than the vehicle's design, defining drone "as unmanned aerial vehicle or aircraft that is operated without the possibility of direct

---

[80] *Id.*
[81] *Id.*

[82] *Id.*

[83] John Wagner, *Bipartisan group of Md. Lawmakers seeks limits on drones, other law-enforcement surveillance*, WASH. POST, Jan. 14, 2014, http://www.washingtonpost.com/local/md-politics/bipartisan-group-of-md-lawmakers-seeks-limits-on-drones-other-law-enforcement-surveillance/2014/01/14/af1c0738-7d38-11e3-93c1-0e888170b723_story.html.

human intervention from within or on the aircraft."[84] As for operation of drones by an agent of the state, Maryland's law restricts such operation unless a warrant for drone surveillance has been issued by a court.[85] If issued, the warrant is only valid for an initial period of 24 hours and must specifically target an individual listed in the warrant.[86] The maximum extension for a warrant of this nature is 30 days.[87]

Most state laws end with this kind of restriction, however Maryland presses forward and goes as far as to restrict the implementation of biometric matching technology or facial recognition software on any non-target individuals, and also explicitly prohibits agents from equipping drones with a weapon.[88] Warrantless use of drones are permitted only in the extreme circumstances, such as an emergency involving the immediate danger of death or serious physical injury, conspiratorial activities threatening the national security interest, or conspiratorial activities characteristic of organized crime.[89] The law further allows for oversight of drone use by requiring agencies to initiate investigative proceedings if an abuse of drone use or violation of this law is suspected.[90] Also, in June of each year agents who have used drones in the previous year must report and make public on the agencies website each time the agent used a drone.[91] No laws effect the private operation and use of drones by private individuals or companies.

---

[84] H.R. 847, 431st Gen. Assemb., Reg. Sess. (Md. 2014).

[85] *Id.*

[86] *Id.*

[87] *Id.*

[88] *Id.* at §E (1-2); (G).

[89] *Id.* at §H(1)(I)(1)(A-C).

[90] *Id.*

[91] H.R. 847, *supra* note 84.

F. Montana

Proposed legislation in Montana seeks to prohibit the collection of data by unmanned aerial vehicles with the use of sensors or other recording devices such as cameras, microphones, thermal detectors, chemical detectors, radiation gauges, or wireless receivers.[92] This is not limited to government agents, but any person operating a UAV within the state.[93] A violation of this law can lead to a maximum $500 fine and not more than 6 months in a county jail.[94] No evidence obtained in violation of this law is admissible in a court of law.[95] Peace officers within the state are prohibited from operating drones for surveillance of an individual unless authorized by a court ordered warrant.[96] If a state or federal agency chooses to implement drones strictly for monitoring of public lands or international borders, then no warrant is needed.[97]

G. Oregon

Oregon's drone laws are primarily crafted to allow for the use of drones by government entities within the state in very limited circumstances, with most uses being prohibited.[98] Not only is evidence inadmissible when gathered by the unlawful use of drones, but such evidence is also not available to establish probable cause or reasonable suspicion to believe that an offense

[92] S.B. 196, 2013 Sen., Reg. Sess. (Mont. 2013).

[93] *Id.*

[94] *Id.*

[95] *Id.*

[96] *Id.*

[97] *Id.*

[98] *See* H.R. 2710, 77th Leg. Assemb., Reg. Sess. (Or. 2013).

has been committed. [99] Drones are only available to law enforcement agencies for surveillance purposes if a court of law issues an appropriate warrant, or when police possess probable cause to believe a crime has, is, or is about to be committed. However if exigent circumstances exist, whereby obtaining a warrant for the use of a drone would be unreasonable, then these law enforcement agencies may circumvent the warrant requirement.[100] Appropriate use of drones under HB 2710 include search and rescue activities, assisting individuals in emergency situations, during a state of emergency as declared by the Governor, for reconstructing crime scenes, or for training law enforcement agencies.[101]

Oregon's law further defines the use of drones by public bodies, defined as state government bodies, local government bodies and special government bodies are prohibited from operating drones in Oregon airspace unless registered with the Oregon Department of Aviation.[102] Registration of possession of drones requires the name of the public body, name and contact information of the individuals operating the drone, identifying information for the drone, and further requires annual reporting of drones use and purpose of use in the preceding year.[103] Unless approved by the Federal Aviation Administration, all data and evidence gathered by drones operated by public bodies is inadmissible in a court of law.[104]

Legislators even went as far to explicitly prohibit the use of weaponized drones by public bodies, including a drone capable of firing a bullet, projectile, directing a laser, or otherwise

[99] H.R. 2710, 77th Leg. Assemb., Reg. Sess., § 2(2)(b) (Or. 2013).
[100] H.R. 2710, 77th Leg. Assemb., Reg. Sess., § 3(1)(b) (Or. 2013).

[101] H.R. 2710, 77th Leg. Assemb., Reg. Sess., §§ 4-7 (Or. 2013).

[102] *§ 174.109 Public Body Defined*, OREGONLAWS.ORG, http://www.oregonlaws.org/ors/174.109 (last visited April 10, 2015).

[103] H.R. 2710, 77th Leg. Assemb., Reg. Sess., §8 (5)-(6) (Or. 2013).

[104] H.R. 2710, 77th Leg. Assemb., Reg. Sess., § 11 (Or. 2013).

being used as a weapon.[105]Concerning individuals within the state, Oregon's law makes it a Class A felony for anyone to cause a drone to fire a bullet or projectile, direct a laser, cause a drone to be flown into another aircraft, or gain control of a drone operated by the FAA or the armed military services – constituting a Class C felony.[106]

Civil remedies allowed under this law focus on individuals who interfere with or take control of a drone licensed by the FAA or operated by the Armed Services entitle the operator of the drone to damages of not less than $5,000 and reasonable attorney's fees.[107] Unlike other states, Oregon has also looked to protect landowners who don't want drones flying over their property. When an operator has flown their drone over a landowner's property at an altitude of less than 400 feet, and has been informed by the landowner not to fly their drone over the landowner's property, the landowner may then bring a civil action for treble damages and injunctive relief.[108] Attorney's fees may be collected if the damages claimed are not in excess of $10,000.[109] Finally, this law is applicable to the entire state and prohibits local legislators from enacting laws affecting the use of drones in Oregon.[110]

H. Tennessee

[105] H.R. 2710, 77th Leg. Assemb., Reg. Sess., § 10 (Or. 2013).
[106] *Id.* at §13.

[107] *Id*. at §14.

[108] Or. H.R. 2710, § 15. H.R. 2710, *supra* note 98, § 15.

[109] *Id.*

[110] *Id.* at §17.

Passed in May of 2013, Tennessee enacted the Freedom from Unwarranted Surveillance Act which seeks to regulate the use of drones within the state.[111] This law identifies drones by their operational capabilities, which are defined as "a powered, aerial vehicle that: (A) does not carry a human operator; (B) Uses aerodynamic forces to provide vehicle lift; (C) Can fly autonomously or be piloted remotely; (D) Can be expendable or recoverable; and (E) Can carry a lethal or nonlethal payload."[112] The law focuses only on the use of drones by law enforcement agencies, strictly prohibited such use in all situations except to counter a high risk of a terrorist attack as determined by the United States Secretary of Homeland Security, by issuance of a search warrant, or if the law enforcement agency determines the use of a drone is needed to prevent imminent danger to life.[113] If violated, aggrieved parties my initiate a civil action for all appropriate relief, and evidence gathered in violation of this law is inadmissible in a court of law.[114] Tennessee leaves private operators of drones unregulated.

I. Texas

Texas legislature finalized state drone laws as of May 24, 2013, restricting the allowable image collection methods by unmanned aerial vehicles.[115] The law makes no reference to other uses of unmanned aerial vehicles, but rather attempts to protect the reasonable privacy rights of Texans. Such images include "any capturing of sound waves, thermal, infrared, ultraviolet,

[111] S. 796, 108th Gen. Assemb., Reg. Sess. (Tenn. 2013).

[112] S. 796, 108th Gen. Assemb., Reg. Sess., §1(b)(1)(A-E), (Tenn. 2013).

[113] *Id.* at § 1 (d)(1-3).

[114] *Id.* at § 1 (e), (f).

[115] Benjamin Minegar, *Texas Legislature Gives Final Approval to Drone Legislation*, May 27, 2013, JURIST, http://jurist.org/paperchase/2013/05/texas-lawmakers-give-final-approval-to-drone-legislation.php; *See* TEX. GOV'T CODE ANN. 912 (West 2013).

visible light, or other electromagnetic waves, odor, or other conditions existing on or about real property or an individual located on that property."[116] No violation occurs if the operator of the drone previously received express consent from the landowner to capture images of the property.[117] Exceptions to the law include issuance of a valid search warrant, law enforcement officers in pursuit of an individual with probable cause to believe the suspect has committed a felony, fire suppression or rescue of a person whose life is in imminent danger, real property within 25 miles of the United States border for the purpose of enforcing border laws, if the image is captured without magnification or other enhancement from no more than 6 feet above the ground, or if the image is taken of public property or of an individual on that public property.[118] Any such violation is a categorized as a Class C Misdemeanor, punishable by a fine of not more than $500.[119]

Violations rise to the level of a Class B misdemeanor if images obtained in violation of Section 423.002 if "a person possesses, discloses, displays, distributes, or otherwise uses" the image.[120] Conviction of a Class B felony can lead to a fine of not more than $2,000 and "confinement in jail for a term not to exceed 180 days."[121] It is an affirmative defense to this violation if the owner of the image destroyed the image as soon as they became aware that it was obtained in violation of Section 423.[122] Further, only images conforming to Texas's law are

---

[116] TEX. GOV'T CODE ANN. §423.001 (West 2013).
[117] TEX. GOV'T CODE ANN. §423.002 (West 2013).

[118] TEX. GOV'T CODE ANN. §423.002 (c)(1)-(6) (West 2013).

[119] Tex. Penal Code § 12.23.

[120] TEX. GOV'T CODE ANN. § 423.004 (West 2013).

[121] TEX. PENAL CODE ANN. § 12.22 (West 2013).

[122] TEX. GOV'T CODE ANN. § 423.004(d) (West 2013).

eligible for disclosure purposes, thus any unlawfully obtained image is exempt from legal discoverable means.[123] Any person found to be the subject of an illegal obtained image under Section 423 is entitled to file a civil suit against the operator of the unmanned aerial vehicle, whereby a $5,000 fine and reasonable attorneys' fees can be assessed for each image of the plaintiff or the plaintiff's property which has been "captured, possessed, disclosed, displayed, distributed, or otherwise used."[124]

J. Virginia

It seems Virginia is poised to wait and see how other states approach and enact drone regulations, as bills passing through both the House (H 2012) and Senate (S 1331) do not attempt to restrict or prohibit any specific uses of unmanned aerial vehicles within the state.[125] Instead legislators simply imposed a state-wide moratorium on the utilization of unmanned aircraft systems prior to July 1, 2015 by state government and law enforcement agencies.[126] As Section 2 of both bills indicate, states agencies are required to develop model protocols for the use of unmanned aircraft systems by law-enforcement agencies, further giving evidence that legislators still have yet to determine how to address unmanned aerial vehicles operations in the state.[127] Exceptions to the moratorium apply in instances where the activation of an Amber, Senior, or Blue alert has been issued, where an unmanned aircraft system is determined to be necessary to

---

[123] 2013 Tex. Sess. Law Serv. Ch. 1390 (H.B. 912) (West).
[124] 2013 Tex. Sess. Law Serv. Ch. 1390 (H.B. 912) (West).

[125] *See generally*, S.B. 1331, Reg. Sess. (Va. 2011); H.B. 2012, Reg. Sess. (Va. 2013).

[126] *Id.*

[127] S. 1331, Gen. Assemb., Reg. Sess. (Va. 2013); H. 2012, Gen. Assemb., Reg. Sess. (Va. 2013).

alleviate an immediate danger to any person, or for training exercises related to such uses.[128] No weaponized drones are allowed within the state.[129]

IV. WHY DRONE LAWS ARE NEEDED

When looking at state and federal regulation of privately operated UAS, it is clear that consideration for the security and privacy interests of citizens is far from sufficiently addressed when considering the capabilities of UAS in a quickly evolving marketplace. For just $300, a civilian can purchase and operate a Wi-Fi connected drone capable of recording streaming 720p resolution footage from a front facing and downward facing camera directly to an individual's electronic device.[130] Accessories available just for this model include extended-life batteries, flight recorders, controllers with built-in screens broadcasting real-time footage during operation, and even OLED glasses worn by the operator, giving in-flight vision to the operator.[131] While the technology is impressive, the privacy implications are unnerving. Even with this relatively inexpensive and basic drone, neighbors or local citizens in possession of this technology now have the ability, without express legal restriction beyond general FAA guidelines, to freely operate their drone in airspace not exceeding 400 feet above the ground.

And not only can these individuals operate the drone overhead, but they have the ability to record streaming video footage and capture still images without first obtaining written consent by those in the videos or pictures. While state regulations have sought to restrict governmental

---

[128] S. 1331, Gen. Assemb., Reg. Sess. (Va. 2013); H. 2012, Gen. Assemb., Reg. Sess. (Va. 2013).

[129] *Id.*

[130] *Parrot AR.Drone 2.0 Elite Edition Quadricopter - Wifi - Free App iOS & Android - Record HD 720p movies - Sand: Electronics*, AMAZON, http://www.amazon.com/Parrot-AR-Drone-Elite-Edition-Quadricopter/dp/B00FS7SSD6/ref=sr_1_2/182-5225229-8894448?ie=UTF8&qid=1394733569&sr=8-2&keywords=parrot+drone (last visited Mar. 1, 2015).

[131] *AR.Drone 2.0. Parrot new wi-fi quadricopter*, PARROT, http://ardrone2.parrot.com/ (last visited Mar. 1, 2015).

use of drone surveillance, individuals implementing drones for such purposes have yet to be directly addressed, thus leaving the door open for anyone with a drone to essentially spy on anyone within operating range. With a click of a button, these recorded videos can be posted on popular internet sites such a YouTube for the entire world to view. For more criminally minded individuals, drones could provide a quick and efficient way to scope out the property of others, determine if homeowners are home, or conduct reconnaissance prior to breaking and entering the property. With drone prices steadily decreasing as the market expands, this may provide a cheap and reliable way for burglars to gather information about a home and surrounding property without physically entering the property. Since drone registration and operation requirements are yet to be implemented, an operator whose drone is discovered hovering over the land of another need only quickly fly the drone back to their operating position, or even allow the drone to be captured in lieu of detection or arrest.

Finally, individuals have already shown that drones are capable of transporting and firing weapons with a fairly high degree of accuracy. For instance, one individual has successfully mounted a fully automatic paintball gun to a drone, and is able to aim and position the gun through real-time streaming video footage.[132] While not fatal, the use of paintballs armed with pepper spray could potentially incapacitate a victim prior to a theft or assault by the drone operator. Unlike drones armed with registered weapons, tracing the attacker would likely prove extremely difficult considering the availability of drones and potential they have for being manipulated. In instances where individuals choose to instead arm their drone with a firearm, such as a small pistol or light machine gun, a drone operator may now carry out a fatal attack without physically being present.

[132] Casey Chan, *An Awesome Guy Made a Flying Drone Armed with a Paintball Gun*, GIZMODO (Dec. 12, 2012, 11:00 PM), http://gizmodo.com/5968058/an-awesome-guy-made-a-flying-drone-armed-with-a-paintball-gun.

With advancing technology and predicted market explosion of civilian owned drones, the list of possible drone uses is seemingly endless.[133] Fortunately legislators are currently in a position to develop appropriate policy responses before civilians become victim to the whims of unregulated drone operators. The FAA is actively researching appropriate regulations, and Advisory Circular 91-57 is good start, but is in need of clear and unambiguous operator flight guidance and procedure to assure the safety of others within the vicinity of a drone. This would help operators coordinate flights to avoid in-air collisions, and would likely serve as an educational tool to make operators aware of various conditions which could place a drone in a potentially harmful situation.

If drones gain popularity as predicted, it would even seem appropriate for the FAA, or individual states (if granted by the FAA), to enact licensing and registration requirements to properly operate a drone beneath the 400 foot Federal limit. Not only would individuals gain useful information regarding the operation of their drone, but authorities would also be aware of who is operating drones and who possesses a drone. Similar to the registration of firearms in various states, serial numbers and descriptions of the drone would likely help deter would-be criminals from spying on or attacking fellow citizens.

Instead of outright bans on drones, registration requirements would enhance operator responsibility, safety, and liability for others who are injured by the operation of a drone. In addition, weaponized drone bans similar to those enacted in Virginia and Oregon will likely gain popularity across the county as legislators become aware of potential airborne attacks. In an age where random mass shootings are unfortunately becoming commonplace, the argument against weaponized drones seems to be fairly straightforward, in that realistic need and use of a

---

[133] Anderson, *supra* note 2.

weaponized drone hardly comes close to outweighing the potential for disaster. Similar to prohibitions on spring-loaded firearms, or booby traps, the justification for protection of property will not overcome the value of life. Further, similar to such firearm contraptions, the lack of physical presence and threat to the landowner reinforces the argument that no imminent danger to life or body was present to legally authorize the use of force by the land owner.

CONCLUSION

At this point in time American citizens need not panic or fear that an attack will be conducted by a drone operated by another citizen. Yet citizens should be aware that drone technology is rapidly developing and becoming widely available without regulations in place to limit the who, when, where, why, and how of private drone operation. Fortunately both State and Federal governments are turning their attention to drones and addressing the issue, but much research and debate still remains to be undertaken. Hopefully within the near future the knowledge gained from FAA test sites will provide enough information for lawmakers to make adequate and appropriate policy decisions regarding the operation of drones within society.

SYRACUSE JOURNAL OF SCIENCE & TECHNOLOGY LAW

VOLUME 31 2014-2015 ARTICLE 8, PAGE 216

THE EUROPEAN UNION'S GENERAL DATA PROTECTION REGULATION: HOW WILL IT AFFECT NON-EU ENTERPRISES?[1]

By: Manu J. Sebastian

INTRODUCTION

In a world where technology is ever changing and personal data is being processed and saved at every turn, corporations must be held accountable for the data they collect, store, and use.[2] The consumer truly does not understand the levels of data capture and retention that corporations employ, and the European Union's ("EU") government is on a mission to ensure that its citizens are protected because it believes personal data protection is a fundamental right

[1] In the summer of 2013, the author worked for Morgan Stanley Capital Investments (MSCI), a major international finance technology firm, in London. His long-term project focused on assisting their Europe, Middle East, and Asia Legal Department in proactively determining how the GDPR would affect the enterprise as a whole. He learned a great deal during his time at MSCI and is grateful to have had the opportunity to work so closely with the talented members of the team. Thank you to Jamie Pawliczek, Christopher Harte, Olga Pulickal, and Sunil Desaur. Secondly, the author would like to give further acknowledgement and thanks to Dean Christian Day of Syracuse University College of Law for his direction, encouragement and advisement and to Dean Aviva Abramovsky of Syracuse University College of Law for her support. Finally, the author would like to extend special thanks to Ms. Abigail L. Reese and the Sebastian Family for their support.

[2] *Data Protection Debate with Jan Philipp Albrecht & Pat Walshe*, VIEUWS (Oct. 17, 2013), http://www.vieuws.eu/ict/data-protection-debate-with-jan-philipp-albrecht-mep-pat-walshe-gsma/ [hereinafter *Data Protection Debate*].

that all people should enjoy.[3] The EU created the General Data Protection Regulation ("GDPR") in an attempt to protect data without detrimentally inhibiting cross-border data flow.[4]

The GDPR is in its final stages of adoption and corporations around the world are working to preemptively establish controls within their internal structures in order to be compliant.[5] These new changes will protect personal data on a level that has never before been seen, but it will come at a great cost to the consumer. The data that is being protected moves far beyond identification numbers and medical data. The GDPR seeks to protect names, phone numbers, addresses, economical data, cultural identity, racial origin, social identity, profiling data, and online identifiers such as IP address and location data, on top of the normal protections of health data and biological samples.[6] The regulation is based on the notion that every single person has the right to have his personal data protected and it protects all people in the EU.[7] These new changes make us ask a very important question: How exactly will Non-EU enterprises be affected?

The changes being proposed not only affect corporations based within the EU, but also affect any corporation that is looking to do business with a person in the EU.[8] International

---

[3] *See Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individual with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation): Compromise Amendments on Articles 1-29*, COM (2012) 0011 (Oct. 7, 2013) [hereinafter *Amended GDPR Art. 1-29*].

[4] *See Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard To the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, COM (2012) 11 final (Jan. 25, 2012) [hereinafter *Proposed GDPR*].

[5] *Data Protection Debate*, *supra* note 2.

[6] *Amended GDPR Art. 1-29*, *supra* note 3, art. 9.

[7] *Proposed GDPR*, *supra* note 4, at 19 ¶ 11.

[8] *Id.*

corporations have an economic need for transborder data flow.[9] As a result, most businesses will be affected, especially those within communications, finance, utilities, construction, medical, transportation, and business services.[10] Additionally, any international corporation that uses a credit card could be affected.[11] Non-EU corporations whose websites use EU Member States' currencies or EU Member States' languages will be viewed as targeting people in the EU.[12] The ramifications of the GDPR are great because it affects the entire global trading system and almost every international enterprise in the world.[13]

To illustrate these issues in the simplest way, we can consider any non-EU corporation that sells a product to a person in the EU. People who are the subject of the protected data are known as Data Subjects and all corporations that collect and process data are labeled Data Controllers ("Controllers") and Data Processors ("Processors").[14] The Data Subject in the EU would place a purchase with the international corporation (an "Enterprise") using their personal information including their name, telephone, and address. Because the EU resident is the buyer entering personal data, the buyer is known as the Data Subject.[15] The Enterprise would be the

---

[9] Press Release, Joint Statement on GDPR (Oct. 16, 2013), *available* at http://www.gsma.com/gsmaeurope/wp-content/uploads/2013/10/Joint-Association-Statement-on-GDPR-161013EP.pdf.

[10] EUROPEAN CENTRE FOR INTERNATIONAL POLITICAL ECONOMY, THE ECONOMIC IMPORTANCE OF GETTING DATA PROTECTION RIGHT: PROTECTING PRIVACY, TRANSMITTING DATA, MOVING COMMERCE, U.S. CHAMBER OF COMMERCE (2013) [Hereinafter ECIPE] *available at* https://www.uschamber.com/sites/default/files/documents/files/020508_EconomicImportance_Final_Revised_lr.pdf.

[11] *Id.* at 5.

[12] *Proposed GDPR*, *supra* note 4, art. 3(2)(a); Briefing Paper on the Proposed General Data Protection Regulation (GDPR) from GSMA Europe, ETNO, ECTA and Cable Europe 4 (Sept. 2012), http://www.gsma.com/gsmaeurope/wp-content/uploads/2012/09/Briefing-Paper-on-Applicable-Law.pdf.

[13] U.S. CHAMBER OF COMMERCE, *supra* note 10.

[14] *See Proposed GDPR*, *supra* note 4.

[15] *Key Definitions of the Data Protection Act*, INFO. COMMISSIONER'S OFF., http://ico.org.uk/for_organisations/data_protection/the_guide/key_definitions (last visited Apr. 2, 2015).

Controller because it determines the purpose and manner in which the personal data is used.[16] As most of the Data Subject's information would be protected under the GDPR, any time the information is transferred to another enterprise or subsidiary within the supply chain, the initial Enterprise would have to ensure that the next enterprise that receives the information complies with the GDPR. These third party enterprises along the chain would be known as Processors since they process the data on behalf of the Controller.[17] Under the GDPR, the transaction would now require the seller to ensure that each entity involved in the supply chain, as well as enterprises like the customer service enterprise, the credit card machine enterprise, the credit card processing enterprise, the warehouse enterprise, the packaging enterprise, the transportation enterprise, and the delivery enterprise, to not only protect the Data Subject's data, but also have the Data Subject consent explicitly and specifically to each entity having his or her data.

Each enterprise involved in the simple transaction would have to be approved by a Data Protection Authority ("DPA").[18] The DPAs could be situated in a number of locations due to the fact that each enterprise involved could be from a different country and each country would have its own DPA. Non-EU entities would have to find some other way to be approved using some other compliance tool and with the way the GDPR is currently written, their options are extremely limited.[19] The amount of money that corporations would spend on the process of complying with the GDPR would squeeze many smaller international enterprises into solely domestic businesses or force them completely out of business.[20] Larger non-EU enterprises with

---

[16] *Id.*

[17] *Id.*

[18] *See Proposed GDPR*, *supra* note 4.

[19] *Id.*

enough income would be required to acquire data processing capacities within the EU.[21] Inevitably, enterprises will be compelled to pass the cost for the additional services associated with the transaction to the consumer, hindering international trade and raising the cost for the consumer.

The GDPR has the potential to completely stop the flow and portability of data between EU and Non-EU countries.[22] It has created a huge outcry from both corporations and government organizations and resulted in the proposal of almost 4,000 amendments to the initial General Data Protection Regulation.[23] While it is important to protect the data of all the Data Subjects in the world, this attempt to balance the increase in data protection and promote the free transborder flow of data portends to have dire consequences on corporations, especially American enterprises that do business in the EU.[24]

This article aims to explain the GDPR to the reader and analyze its effect on American and other non-EU enterprises, as well as its effect on international law and international commerce. It begins by briefly explaining the process of creating the GDPR and the regulation's history as it moves along the legislative path towards ratification. The article will then compare the GDPR and the initial 1995 Data Protection Directive to determine the changes between the two in order to identify the areas that American and non-EU enterprises must focus on to proactively prepare for the GDPR's ratification. The main effect on non-EU enterprises is the

---

[20] *ICC Comments On EU General Data Protection Regulation Issues*, INT'L CHAMBER OF COM. (Jan. 15, 2013), http://www.iccwbo.org/Advocacy-Codes-and-Rules/Document-centre/2013/ICC-comments-EU-Gen-DP-Reg-Issues/.

[21] ECIPE, *supra* note 10.

[22] *Id.*

[23] Memorandum from the Eur. Comm'n, LIBE Committee Vote Backs New EU Data Protection Rules (Oct. 22, 2013), *available at* http://europa.eu/rapid/press-release_MEMO-13-923_en.htm.

[24] INT'L CHAMBER OF COM., *supra* note 20.

GDPR's territorial reach that now places all international firms under its jurisdiction. This article will compare the different compliance tools non-EU enterprises currently use in order to comply with the Data Protection Directive's requirements and discuss why the GDPR's removal of these tools will lead to dire consequences for everyone involved. Finally, this article will suggest possible alternatives to the current compliance tools in order to ease the transition of complying with the GDPR.

I. THE LEGISLATIVE PROCESS

The EU consists of twenty-eight different countries known as Member States.[25] It has a government consisting of three different branches: the European Parliament, the Council of the European Union, and the European Commission, together known as the EU Institutions.[26] The European Parliament is one of the legislative branches and consists of 732 elected representatives from the Member States based on population. [27] The Members of Parliament are elected for five-year terms and divided into specialized committees and delegations based on their knowledge and expertise. [28] The Council of the European Union is another legislative branch consisting of representatives from the governments of the Member States with its composition dependent on the subjects on the agenda. [29] The Presidency of the Council is held

[25] *EU Member Countries*, EUR. UNION, http://europa.eu/about-eu/countries/member-countries/index_en.htm (last visited Apr. 2, 2015).

[26] *Process and Players,* EUR-LEX, http://old.eur-lex.europa.eu/en/droit_communautaire/droit_communautaire.htm#2 (last visited Apr. 2, 2015).

[27] *Id.*
[28] *Id*.

[29] *Id.* Keep in mind that the Council of the European Union is not to be confused with the European Council. While the Council of the European Union is a legislative body, the European Council actually consists of the Heads of State of the Member States and the President of the European Commission. The President of the European Council, who is considered the President of the European Union as a whole, leads the European Council.

in a six-month rotation by each Member State.[30] At the time of the initial GDPR proposal, the Presidency was held by Ireland; it then went to Lithuania, then Greece, and will soon be turned over to Italy.[31] The European Commission is the executive branch of the EU and consists of one member from each Member State.[32] The members are appointed by the Council for a five-year term and approved by Parliament.[33]

The European Commission has the power to initiate most laws including the GDPR, which was proposed on January 25, 2012.[34] The EU Institutions pass laws in the form of directives and regulations.[35] Directives are broad statutes that allow each Member State to enforce the directive as they see fit and in accordance with their state laws.[36] Regulations are more rigid and uniform and do not allow Member States to interpret them.[37] As the GDPR is a regulation, Member States may not interpret it as they would with a directive. Rather, Member States must adhere to it directly once it is ratified.

The GDPR takes concepts from Directive 95/46/EC ("Data Protection Directive"), which is the current data protection directive passed in 1995,[38] and combines the Member States resulting patchwork of laws in an attempt to create a strict uniform law for the European Union

---

[30] *Id.*

[31] *Council of the European Union*, EUR. UNION, http://europa.eu/about-eu/institutions-bodies/council-eu/index_en.htm (last visited Apr. 2, 2015).

[32] *Process and Players*, *supra* note 26.

[33] *Id.*

[34] *Id.*

[35] *Id.*

[36] *EU Law: Regulations, Directives and Other Acts*, EUR. UNION, http://europa.eu/eu-law/decision-making/legal-acts/index_en.htm (last visited Apr. 2, 2015).

[37] *Id.*

[38] *See* Council Directive 95/46, 1995 O.J. (L 281) 31 (EC).

as a whole.[39] The Data Protection Directive was created to acknowledge the eight Mandatory Data Protection Principles.[40] Personal data must be:

> (1) [P]rocessed fairly and lawfully; (2) obtained only for one or more specified lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes; (3) adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed; (4) accurate and, where necessary, kept up-to-date; (5) not be kept for longer than is necessary for that purpose; (6) processed in accordance with the rights of data subjects under the Data Protection Act; (7) appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data; and (8) not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.[41]

Since Member States were allowed to enforce the directive as they interpreted it, a patchwork of twenty-eight separate data protection laws derived from the Data Protection Directive.[42] The GDPR attempts to combine this patchwork into one unified law and further expand data protections.[43] The concept seems like a good idea on paper but its implementation is much more difficult and detrimental without proper transition, safeguard, and compliance tools.

Once the Commission created the GDPR proposal, it was sent to Parliament and the Council, as well as the Member States' national governments, for review.[44] Almost every entity

---

[39] *See Proposed GDPR*, *supra* note 4.

[40] *Data Protection Principles*, INFO. COMMISSIONER'S OFF., http://www.ico.org.uk/for_organisations/data_protection/the_guide/the_principles?hidecookiesbanner=true (last visited Apr. 2, 2015).

[41] *Id.*

[42] *LIBE Committee Vote on Data Protection Regulation*, VPH INST. (Nov. 11, 2013), http://www.vph-institute.org/news/libe-committee-vote-on-data-protection-regulation.html.

[43] *Id.*

[44] *EU Legislative Process Updates*, WILSON SONSINI GOODRICH & ROSATI, LLP, http://www.wsgr.com/eudataregulation/process-updates.htm (last visited Apr. 2, 2015).

that received the proposal proposed amendments to it. The Irish Presidency of the Council created a new draft incorporating a number of proposed amendments in May of 2013.[45] Four committees within the Parliament, the Legal Affairs Committee, the Internal Market and Consumer Protections Committee, the Industry, Research, and Energy Committee, and The Employment and Social Affairs Committee, submitted additional amendments to The Committee on Civil Liberties, Justice and Home Affairs ("LIBE").[46] LIBE had been delegated to create the final version that was voted on by Parliament.[47] A number of lobbyists from different organizations, including the International Chamber of Commerce ("ICC"), also requested to be heard and submitted their amendments as well.[48] Due to the influx of responses, LIBE postponed its vote on the proposed draft of the Regulation four times since it first received the initial proposal.[49]

When all was said and done, the LIBE committee found itself facing 4,000 proposed amendments, and on October 21, 2013, it finally released its own version of the Regulation, which compromised the 4,000 amendments into 104 amendments.[50] LIBE voted 49-1 to approve this version and it was presented to the rest of Parliament for a vote.[51] To date, the GDPR has gone through a number of further postponements and adjournments.[52] The Member States

---

[45] *Id*.

[46] *Legislative Observatory*, EUR. PARL., http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2012/0011%28COD%29&l=en.

[47] WILSON SONSINI GOODRICH & ROSATI, LLP, *supra* note 44.

[48] INT'L CHAMBER OF COM., *supra* note 20.

[49] WILSON SONSINI GOODRICH & ROSATI, LLP, *supra* note 44.

[50] LIBE Committee Vote Backs New EU Data Protection Rules, *supra* note 23.

[51] VPH INSTITUTE, *supra* note 42.

finally decided to adjourn its implementation until at least 2015 due to the controversy and disagreement surrounding the GDPR.[53]

II. DELTAS FROM DIRECTIVE 95/46/EC

The General Data Protection Regulation differs from the Data Protection Directive in that it: (1) shifts data protection powers from the Member States to Brussels and expands the EU's territorial reach;[54] (2) creates lead supervisory authorities as governmental regulatory agencies and the need for supervisory authorities within enterprises individually;[55] (3) forces greater accountability and responsibility on controllers and processors;[56] (4) defines consent and establishes the rights of data subjects;[57] and (5) specifies a time limit for breach notice and imposes high penalties in the form of monetary sanctions.[58]

A. Powers: The Shift of Control and Expanded Territorial Reach

Above all else, Data Protection will now be enforced through a regulation instead of a directive, meaning all Member States must adhere to the regulation as written with no room for

---

[52] *EU Data Protection Regulation Tracker*, HUNTON & WILLIAMS, http://www.huntonregulationtracker.com/legislativescrutiny/#ScrutinyEUCommission (last visited Apr. 2, 2015).

[53] Kenneth Mullen and Brian Dunefsky, *European Union: On Hold: EU Data Protection Reform Delayed* (Dec. 31, 2013), MONDAQ, http://www.mondaq.com/x/283634/data+protection/On+Hold+EU+Data+Protection+Reform+Delayed.

[54] *Radical Changes to European Data Protection Legislation*, ALLEN & OVERY (Jan. 2012), http://www.allenovery.com/SiteCollectionDocuments/Radical%20changes%20to%20European%20data%20protection%20legislation.pdf.

[55] *Id.*

[56] *Id.*

[57] *Data Protection Debate*, *supra* note 2.

[58] *Id.*

interpretation.[59] The Commission will also have the power to adopt further legislation in order to rectify any issues that may be presented after the Regulation goes into effect.[60] In essence, Member States will relinquish control over data protection in their individual countries. The ratification essentially allows the EU Institutions to determine how data protection is handled throughout the EU as a whole. Since all three branches of the EU government, as well as the European Council, meet in Brussels, it is said that the power behind data protection will move from the Member States to Brussels[61].

Any enterprise that collects data from a person in the EU must adhere to the GDPR.[62] The Data Protection Directive only applied to Controllers within the EU and it only prohibited the transfer of data across borders to countries that did not have "adequate" data protections.[63] The GDPR now expands the territorial reach of the EU government by requiring any Controller, no matter where it is located, to adhere to the GDPR when dealing with a person within the EU.[64] It does not matter if the actual data processing takes place within the EU or outside of its boundaries.[65] This new requirement has the greatest effect on non-EU enterprises and instantly creates the need for all international non-EU enterprises to reconsider how they conduct business with anyone in the EU.

---

[59] Press Release, Council of the Eur. Union, 3260th Council Meeting of Justice and Home Affairs (Oct. 7-8, 2013), *available at* http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/138925.pdf.

[60] *Radical Changes to European Data Protection Legislation*, *supra* note 54.

[61] *Id.*

[62] *Amended GDPR Art. 1-29*, *supra* note 3, art. 3.

[63] Council Directive 95/46, *supra* note 38.

[64] *Amended GDPR Art. 1-29*, *supra* note 3, art. 3.

[65] *Id.*

2. Authorities: Data Protection Authority, the European Data Protection Board, and Data Protection Officers.

The Data Protection Directive mandated that Member States create a number of supervisory authorities within their individual states that would assist in the enforcement of the Data Protection Directive.[66] These supervisory authorities have become known as Data Protection Authorities ("DPAs").[67] The GDPR further clarifies the idea set forth in the Data Protection Directive by instituting the requirement of one lead supervisory authority for Controllers and Processors that have offices in more than one Member State or collect and process data of Data Subjects from more than one Member State.[68] As a result, an international enterprise within multiple jurisdictions now has the ability to use one national DPA to supervise all of its data processing activities throughout all of the enterprise's locations.[69] The main location will be determined by where the main processing activities take place, or in the case of a data processor, where the place of central administration is located within the EU.[70] This simplifies the burden on multi-national corporations *within* the EU, but still does not have any positive effect on non-EU enterprises.

The GDPR furthers the concepts of co-operation and consistency by creating the European Data Protection Board ("EDPB").[71] The EDPB has exclusive jurisdiction to enforce

---

[66] Council Directive 95/46, *supra* note 38, art. 28.

[67] *See Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individual with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation): Compromise Amendments on Articles 30-91*, COM (2012) 0011 (Oct. 17, 2013) [hereinafter *Amended GDPR Art. 30-91*].

[68] *Id.* art. 54a.

[69] *Radical Changes to European Data Protection Legislation*, *supra* note 54.

[70] *Amended GDPR Art. 30-91*, *supra* note 67, art. 54a.

[71] *Id.* art. 64.

the GDPR in a uniform fashion.[72] It will be comprised of one head of each DPA in each of the Member States, the European Data Protection Supervisor,[73] and led by a full-time Chair.[74] The Commission will still have the authority to participate in any of the EDPB's activities and meetings, but the EDPB will act independently and will not seek or take instructions from other bodies in the performance of its tasks.[75] The EDPB shall advise the European Institutions on any questions regarding the application of the GDPR, advise on recommendations and best practices,[76] and create a report every two years regarding data protection in the EU and third countries.[77] The EDPB will become the main EU authority and will oversee the exchange of knowledge and documentation between the DPAs worldwide,[78] including a register of all warnings, breaches, and sanctions that have been collected by the DPA.[79]

To enhance the idea of co-operation and consistency, the GDPR also requires all public authorities to have an independent Data Protection Officer ("DPO") dedicated to ensuring that the data the enterprise uses is protected and the processes used adhere to the GDPR.[80] The DPO will ensure the concept of privacy by design and utilize Privacy Impact Assessments to safeguard personal data. In addition to public authorities, all international enterprises that process the personal data of more than "5,000 Data Subjects in any consecutive 12-month period" or whose

---

[72] *Id.* art. 66; *see also* 3260th Council Meeting of Justice and Home Affairs, *supra* note 59.

[73] *Amended GDPR Art. 30-91*, *supra* note 67, art. 64.

[74] *Id.* art. 69.

[75] *Id.* art. 65.

[76] *Id.* art. 66.

[77] *Id.* art. 67.

[78] *Amended GDPR Art. 30-91*, *supra* note 67, art. 66.

[79] *Id.* art. 52.

[80] *Id.* art. 35.

core activities consist of processing special category data must also have a designated and independent DPO.[81] The concept of a DPO is not new, as the Data Protection Directive allowed enterprises with an independent data protection official to have more freedoms compared to controllers that did not have an independent data protection official.[82]

The major difference is that the GDPR now *requires* a DPO.[83] The effect of this requirement is that enterprises would be forced to create and finance a position within the enterprise's management staff that is accountable solely for the enterprise's data protection responsibilities.[84] In a time where technology can easily capture the information of 5,000 people in a matter of minutes with something so simple as an online form, any enterprise with a website would be forced to create an independent DPO position.[85] Before the GDPR, one person might have had a multitude of responsibilities in a smaller enterprise; now almost every enterprise must find and pay a data protection professional. This could put smaller international enterprises in a compromising situation, as they may barely be able to stay afloat let alone try to now find and employ an individual who is designated solely to protect data.

C. Accountability and Responsibility: Privacy by Design, Maintenance of Documentation, Privacy Impact Assessments, Legitimate Interests, and Shared Responsibility Between Controllers and Processors.

---

[81] *Amended GDPR Art. 1-29*, *supra* note 3, art. 6.

[82] Council Directive 95/46, *supra* note 38, art. 18(2).

[83] *Amended GDPR Art. 30-91*, *supra* note 67. art. 35

[84] *Proposed GDPR*, *supra* note 4. art. 37

[85] *Databases And Data Capture*, BBC, http://www.bbc.co.uk/schools/gcsebitesize/ict/databases/2databasesrev1.shtml (last visited Apr. 2, 2015); *see Top Ten Data Capture Tips*, ADMA, http://www.adma.com.au/connect/articles/top-ten-data-capture-tips/ (last visited Apr. 2, 2015); *see also Methods of Data Capture*, PROCESSFLOWS, http://www.processflows.co.uk/data-capture/methods-of-data-capture/ (last visited Apr. 2, 2015).

For corporations, data collection and processing begins at the creation of a data project. For example, when an enterprise uses a website to market its product to customers, each person that signs up will enter their information into the enterprise's website and this data will then be collected and processed. This endeavor is the enterprise's data collection and processing project. The GDPR requires that enterprises now consider data protection and privacy right from the beginning of the project's creation and inception, known as "privacy by design."[86] The project is designed around the concept of privacy. Privacy by design ensures that data protection is in the forefront of enterprises' data collection and processing efforts.

The Data Protection Directive required that Controllers and Processors notify supervisory authorities before "carrying out any wholly or partly automatic processing operation or set of such operations."[87] As technology advanced since the Data Protection Directive's implementation in 1995, this requirement to notify the DPA has become obsolete. Therefore, the GDPR no longer requires it.[88] In the initial proposal of the GDPR, the notification requirement was replaced with an obligation to maintain documentation of all processing operations.[89] The amended GDPR now only requires effective procedures and mechanisms that focus on identifying risks related to the protection of personal data.[90] This lesser requirement was done in the hopes of lessening the burdens on EU enterprises. Yet, once again, this leniency does not help non-EU enterprises.

---

[86] *Privacy By Design*, INFO. COMMISSIONER'S OFF., http://ico.org.uk/for_organisations/data_protection/topic_guides/privacy_by_design (last visited Apr. 2, 2015).

[87] Council Directive 95/46, *supra* note 38, art. 18.

[88] *Proposed GDPR*, *supra* note 4, art. 18(2).

[89] *Radical Changes to European Data Protection Legislation*, *supra* note 54.

[90] *Amended GDPR Art. 30-91*, *supra* note 67, at recital ¶70.

To comply with this lesser requirement, entities must conduct data protection Privacy Impact Assessments ("PIAs").[91] PIAs are used to analyze "how personally identifiable information is collected, used, shared, and maintained."[92] Enterprises must identify and manage risks, avoid unnecessary costs, avoid loss of trust and reputation, inform media, advocacy groups, and regulatory agencies of the organization's communication strategy, and meet and exceed legal requirements that are set forth by the Data Protection Regulation.[93] PIAs work best when they are implemented at the beginning of the data collection process, especially when the project is in its design stages.[94] This allows the enterprises that utilize the PIA to identify and repair risks before it is too late.[95] PIAs are a proactive tool that ensures compliance with the GDPR. In addition to PIAs, the GDPR also requires a compliance review to be done at least once every two years or immediately when a change in risk presents itself.[96] The documentation from both the PIAs and the compliance reviews must be made available to the appropriate DPA.[97]

In the course of processing personal data, Controllers employ and use Processors to assist in the task. Processors will now be held accountable and have direct obligations just like Controllers.[98] For example, Processors must assist Controllers in Privacy Impact Assessments,

---

[91] *Id.* art. 33.

[92] *Privacy Impact Assessments*, FED. TRADE COMM'N, http://www.ftc.gov/site-information/privacy-policy/privacy-impact-assessments (last visited Apr. 2, 2015).

[93] *See Privacy Impact Assessment Handbook*, INFO. COMMISSIONER'S OFF., *available at* http://www.rogerclarke.com/DV/ICO-2007-V2.pdf (last visited Apr. 2, 2015).

[94] *Id.* at 5.

[95] *Id.*

[96] *Amended GDPR Art. 30-91*, *supra* note 67, art. 33a.

[97] *Id.*

implementing technical and organizational measures, maintaining documentation on processing activities, and keeping the Controller informed at all stages of the data processing.[99] Data Processors must also have prior permission before they appoint a sub-processor, which is a Processor that is employed by another Processor.[100]

According to the GDPR, enterprises must also show that there are "legitimate interests" for collecting and processing data.[101] They must explain the need for transferring data with legitimate reasons explicitly approved by the DPAs.[102] There are many legitimate reasons to collect data, such as the obvious need to know where to send a product to a consumer, but the need to transfer data is less obvious. Legitimate interests to transfer data would include data security or network services, preventing fraud, direct marketing, anonymising or pseudonymising data, or keeping data for historical, statistical, or scientific reasons. [103] The Controller and Processor must meet clear requirements, such as processing in a manner of "reasonable expectation."[104] Thus, they may only process personal data in a way that is reasonably expected by the Data Subject. Any transfer request to a third country requires authorization from the national DPA before the transfer can be processed, and the data subject must be notified of the request.[105]

---

[98] *Radical Changes to European Data Protection Legislation*, *supra* note 54.

[99] *Id.*

[100] *Id.*

[101] *Amended GDPR Art. 1-29*, *supra* note 3, art. 5.

[102] *Radical Changes to European Data Protection Legislation*, *supra* note 54.

[103] *Amended GDPR Art. 1-29*, *supra* note 3, art. 6.

[104] *Data Protection Debate*, *supra* note 2.

[105] Brian Tarran, *EU Civil Liberties Committee Backs 'Right to Erasure' of Data,* RES. (Oct. 22, 2013), http://www.research-live.com/news/government/eu-civil-liberties-committee-backs-right-to-erasure-of-data/4010672.article.

D. The Rights of the Data Subject: Consent Requirements, the Right to Access, and the Right to Erasure.

For the Data Subject, data collection and processing begins with consent. The Data Subject must give clear consent.[106] Clear consent is defined as consent that is freely given and specific.[107] It must be an informed and explicit indication of the Data Subject's wishes.[108] Also, consent must be given using a statement or by a clear affirmative action.[109] Consent must be limited to purpose and the consent will expire when the purpose for which consent was given ceases to exist or the "processing of personal data is no longer necessary for carrying out the purpose for which it was originally collected."[110] The ability to withdraw consent must be as easy as it was to actually give the consent.[111] The Data Subject may withdraw consent at any time and the Controller shall inform the Data Subject if the withdrawal of consent results in termination of services.[112] Data Subject's may also submit complaints free of charge to the DPA.[113]

A Data Subject has a "Right to Access" their protected data that is being processed.[114] Controllers and Processors must respond to any request within forty (40) calendar days.[115] The

---

[106] *Id.*

[107] *Id.*

[108] *Id.*

[109] *Id.*

[110] *Amended GDPR Art. 1-29*, *supra* note 3, art. 7.

[111] *Id.*

[112] *Id*.

[113] *Amended GDPR Art. 30-91*, *supra* note 67, art. 52.

[114] *Amended GDPR Art. 1-29*, *supra* note 3, art. 12.

Data Protection Directive requires that each request inform the Data Subject as to whether data relating to the Subject is being processed, the purpose of the processing, the categories of data concerned, the category of recipients to whom data is disclosed, communication of the data processed, and information as to the logic involved in relation to automatic decisions.[116]

The GDPR expands the "Right to Access" by requiring additional information be presented, such as the period for which personal data will be stored, the existence of the right to request, the right to rectify, the right to erase, the right to object, the right to lodge complaints, and the consequences of the data processing.[117] Controllers may no longer charge a fee for the access request.[118] Also, the time to respond to the request will be lowered to one month and specific forms to request the data will be created.[119] However, Member States will be allowed to introduce exemptions as needed.[120]

The GDPR establishes the "Right to Erasure," which was formerly known as the "Right To Be Forgotten."[121] This right allows a Data Subject to request removal from a Controller or Processor's data capture system.[122] The data includes anything that the enterprise may have collected on their own or any data that the data subject posted "on the Internet themselves."[123]

---

[115] *Id.*

[116] Nigel Parker, *Unregulated Access – The Expanded Right of Access Under the Proposed Regulation*, ALLEN & OVERY 2 (Mar. 2012), http://www.allenovery.com/SiteCollectionDocuments/Unregulated%20access%20-%20The%20expanded%20right%20of%20access%20under%20the%20proposed%20Regulation.pdf.

[117] *Id.*

[118] *Id.*

[119] *Proposed GDPR*, *supra* note 4, art. 12.

[120] *Id.*

[121] Tarran, *supra* note 105.

[122] *Id.*

[123] *Id.*

The enterprise must also "forward the request to others where the data was replicated."[124] The concept seems valid in theory, but in practice it becomes almost impossible to truly erase a subject's data. The newest version of the GDPR presented by the LIBE committee attempts to address the Right to Erasure by allowing a number of exceptions that may assist Controllers while at the same time protect Data Subjects, but the entire concept has its flaws.[125]

Data disseminates at every turn and can become impossible to trace. Enterprises will not have access to public information listed on the Internet and cannot be held accountable for the deletion of that information.[126] Once the enterprise has erased a subject from its systems, the enterprise cannot keep track of the simple fact that the subject's information should have been erased. This leaves enterprises in a "catch-22" situation where they can be sanctioned for contacting someone that they should have erased, yet the enterprise has no way of knowing that the person was supposed to be erased if they cannot store that subject's particular data in order to keep track of those who should have been erased. Also, many enterprises keep servers backed up for multiple years for compliance and legal reasons. So, enterprises would now have to go through all of their backup files in order to ensure that the subject's data is deleted upon request.[127] If the data subject requests their information be deleted but then files a claim against the enterprise later on, the enterprise no longer has any of the data subject's information and will be unable to appropriately combat the claim against them. The intricacies of this concept create a huge financial burden on enterprises.[128]

---

[124] *Id.*

[125] *Amended GDPR Art. 1-29*, *supra* note 3, art. 17.

[126] Parker, *supra* note 116.

[127] *Id.*

[128] *Id.*

The LIBE committee's version of the GDPR attempts to quell this fear by allowing a restricted processing exception if the Controller shows they would need the data for "the purposes of proof."[129] Under the exception, the Controller or Processor would restrict the processing of personal data so that it is not the subject of normal data access.[130] Further, processing operations and personal data could no longer be changed in anyway.[131] This exception essentially invalidates the entire "Right to Erasure" concept as all enterprises could show a necessity to keep data for "the purposes of proof."[132] Therefore, the "Right to Erasure" should be amended to the "Right to Restriction." This would achieve the goal of protecting a Data Subject's personal data from being further disseminated and also assist the Controller in keeping a record of the Data Subject's personal data in order to protect the Controller from any claims that could arise.

E. Breach: Notice and Sanctions

If a breach occurs, the GDPR requires notification without undue delay to the DPA even if the breach was harmless.[133] Undue delay is presumed to be within seventy-two (72) hours and enterprises that do not comply will face sanctions.[134] A breach can be any event or action that would result in an adverse effect on personal data or privacy of a Data Subject including identity theft, fraud, physical harm, significant humiliation, or damaged reputation.[135] The notification

---

[129] *Amended GDPR Art. 1-29*, *supra* note 3, art. 17(4).

[130] *Id.*

[131] *Id.*

[132] *Id.*

[133] *Data Protection Debate*, *supra* note 2; *Amended GDPR Art. 1-29*, *supra* note 3, ¶67.

[134] *Data Protection Debate*, *supra* note 2.

must include a description of the breach including the types of data and number of Data Subjects concerned, the DPO's name and contact information, recommendations on how to mitigate the breach, a description of the consequence of the data breach, and the steps the enterprise has taken to address the breach.[136] The Controller/Processor must keep detailed documentation in regards to the breach including the surrounding facts, its effects, and the remedial action taken.[137]

The Controller must show the DPA that it has implemented sufficient technological protection measures to render the data unintelligible to those not authorized to access it.[138] If the Controller is unable to do so, the enterprise must also notify the Data Subject, whose personal data was breached, without undue delay.[139] The communication must be in comprehensive, clear, and plain language and include the same information that was sent to the DPA in the breach notification.[140]

Corporations can be punished for any inconsistencies through sanctions.[141] Sanctions will take into account the nature, gravity, and duration of incompliance, the intentional or negligent character of the infringement, the degree of responsibility, the previous breach history, the degree of cooperation with the DPA, the level of damage, the actions taken to mitigate the breach, the financial benefit gained or the loss avoided by breach, the degree of technical or organizational measures implemented to prevent breaches, and any other aggravating or

---

[135] *Amended GDPR Art. 1-29*, *supra* note 3, ¶67.

[136] *Amended GDPR Art. 30-91*, *supra* note 67, art. 31.

[137] *Id.*

[138] *Id.* art. 32.

[139] *Id*.

[140] *Amended GDPR Art. 30-91*, *supra* note 67, art. 32.

[141] *Id.* art. 79.

mitigating factors.[142] The possible sanctions include written warnings, regular and periodic audits, fines of €100,000,000, or up to five percent (5%) of their worldwide turnover.[143] These high and unfair monetary sanctions could easily cripple international enterprises if they are handed out arbitrarily.

III. TRANSFERS TO THIRD COUNTRIES OUTSIDE OF THE EU

The Data Protection Directive and the GDPR both prohibit the transfer of personal data outside of the EU to third countries that do not have "adequate" protections and safeguards.[144] Adequacy is determined by a number of factors including the third countries': (1) rule of law that allows effective administrative and judicial redress for Data Subjects; (2) independent supervisory authority with sufficient sanctioning powers; and (3) legally binding instruments and conventions with regard to personal data protection.[145] At the moment, the only countries outside of the EU that are considered to adequately safeguard personal data are Andorra, Argentina, Canada Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland, and Uruguay.[146]

Other non-EU enterprises currently use compliance tools such as Safe Harbor, EU Model Clauses, and Binding Corporate Rules to comply with the current Data Protection Directive.[147]

---

[142] *Id.*

[143] LIBE Committee Vote Backs New EU Data Protection Rules, *supra* note 23.

[144] *Amended GDPR Art. 30-91*, *supra* note 67, art. 41.

[145] *Id.* art. 41(2).

[146] ECIPE, *supra* note 10.

[147] Jeremy M. Mittman, *EU Working Party Adopts Model Application Form for Binding Corporate Rules,* PROSKAUER (Mar. 8, 2007), http://privacylaw.proskauer.com/2007/03/articles/european-union/eu-working-party-adopts-model-application-form-for-binding-corporate-rules/.

These tools allow enterprises outside of the EU the ability to comply with the Data Protection Directive without creating unnecessary restrictions on them from a government that has limited jurisdiction over them.[148] Without these compliance tools, it would be nearly impossible for non-EU enterprises to conduct business and trade with people in the EU because the Data Protection Directive forbids the dissemination of personal data outside of the EU to any third party that does not have "adequate" data protection safeguards.[149]

The US-EU Safe Harbor Framework Agreement ("Safe Harbor") was created to respect the data protection established by the Data Protection Directive while still allowing uninterrupted flows of data between the United States and the EU.[150] The seven principles of Safe Harbor are notice, choice, onward transfer, access, security, data integrity, and enforcement.[151] The Safe Harbor principles directly correlate to the Data Protection Directives data protection principles.[152] American enterprises participating in Safe Harbor self-certify that they are providing "adequate protection" for transferring personal data from the EU to the US.[153] The

---

[148] *Id*.

[149] *Id.*

[150] Damon Greer, *Safe Harbor May Be Controversial in the European Union, But It Is Still the Law*, THE PRIVACY ADVISOR (Aug. 27, 2013), https://www.privacyassociation.org/publications/safe_harbor_may_be_controversial_in_the_european_union_but_it_is_still_the; W. Gregory Voss, *Preparing for the Proposed EU General Data Protection Regulation: With or Without Amendments,* A.B.A. (Nov. 19, 2012), http://apps.americanbar.org/buslaw/blt/content/2012/11/article-02-voss.shtml.

[151] *Federal Trade Commission Enforcement of the US-EU and US-Swiss Safe Harbor Frameworks*, FED. TRADE COMM'N (Dec. 2012), https://www.ftc.gov/tips-advice/business-center/guidance/federal-trade-commission-enforcement-us-eu-us-swiss-safe-harbor.

[152] Amy Worley, *FTC Serious About Safe Harbor Framework Enforcement*, MONDAQ (Feb. 10, 2014), http://www.mondaq.com/unitedstates/x/291886/data+protection/FTC+Serious+About+Safe+Harbor+Framework+Enforcement.

[153] Belinda Doshi and Robyn Chatwood, *European Union: Is "Safe Harbor" No Longer Safe? EU to Review Regime for Personal Data Transfers to the US*, MONDAQ (Aug. 9, 2013),

process is a self-regulatory framework that is enforced by the U.S. Federal Trade Commission ("FTC").[154] There are more than 4,000 entities currently using the Safe Harbor program and over seventy (70) new applications every month.[155]

Safe Harbor only applies to enterprises under the jurisdiction of the FTC and the Department of Transportation ("DoT").[156] This means that enterprises within finance (banks, investment houses, credit unions, and savings & loans institutions), telecommunications, labor, non-profit, agriculture, and meat processing are not automatically eligible to use Safe Harbor as a compliance tool in regards to data protection.[157] It can be argued that Safe Harbor has helped to increase the interest in privacy protection in the U.S. since its inception, but the self-regulatory aspect has been under constant fire and criticism.[158] In fact, the European Parliament released a draft report and resolution that looks to establish a "European digital habeas corpus" that would suspend Safe Harbor.[159] Safe Harbor's demise would be detrimental to the 4,000 entities that use it, as well as the new enterprises looking to expand into the international market.

Incorporating EU Model Clauses within contracts is another way to comply with the Data Protection Directive.[160] They allow the transborder transfer of data and hold the parties involved

---

http://www.mondaq.com/x/256996/data+protection/Is+Safe+Harbor+No+Longer+Safe+EU+To+Review+Regime+For+Personal+Data+Transfers+To+The+US.

[154] Damon Greer, *Safe Harbor – A Framework that Works*, 1 INT'L DATA PRIVACY L. 143, 146 (2011).

[155] *Id.*

[156] *Eligibility for Self-Certification,* U.S. DEPT. OF COM., http://export.gov/safeharbor/ (last updated July 1, 2013).

[157] *Id.*

[158] *Safe Harbor – A Framework that Works*, *supra* note 154.

[159] Donald Aplin, *12 Companies Settle FTC Charges Of Falsely Asserting U.S.-EU Safe Harbor Compliance*, BLOOMBERG BNA (Jan. 27, 2014), http://www.bna.com/12-companies-settle-n17179881618/; *see also Draft Report On The Electronic Mass Surveillance of EU Citizens,* 2013/2188 (INI), (Dec. 23, 2013), *available at* op.bna.com/pl.nsf/r?Open=dapn-9f5kyk.

accountable.[161] Controllers must incorporate standard contractual clauses into their service agreements that are approved by the Information Commission.[162] The clauses are based upon the Mandatory Data Protection Principles.[163] Each clause must be entered exactly as written otherwise the Information Commission will not guarantee that adequate safeguards are provided and the effectiveness of the modification may be challenged.[164] Also, the data exporter and importer must accept liability for any breach and cross indemnify each other to ensure that one of them would be held responsible in case of a data breach.[165] Overall, these clauses are an attempt to protect data through contractual means and any deviation would be considered a breach of contract.[166] The downside behind EU Model Clauses is that they require hundreds of separate contracts in order for large companies to comply because each transaction would require a separate contract with an EU Model Clause.[167]

Binding Corporate Rules ("BCRs") are legally binding corporate codes of conduct that allow data handling systems to be EU-compliant.[168] An international enterprise uses BCRs to

---

[160] Memorandum from the Eur. Comm'n, Decision Updating the Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Non-EU Countries PINCITE (Feb. 5, 2010), *available at* http://ec.europa.eu/justice/policies/privacy/docs/modelcontracts/memo_10_30_en.pdf [hereinafter *Decision Updating the Standard Contractual Clauses*].

[161] *Id.*

[162] *Id.*

[163] *Model Clauses for Transferring Personal Data Overseas: An Overview*, PINSET MASONS LLP, http://www.out-law.com/page-8172 (last updated May 2010).

[164] *Model Contract Clauses: International Transfers of Personal Data*, INFO. COMMISSIONER'S OFF., http://www.ico.org.uk/~/media/documents/library/Data_Protection/Detailed_specialist_guides/model_contract_clauses_international_transfers_of_personal_data.ashx (last visited Apr. 2, 2015).

[165] *Decision Updating the Standard Contractual Clauses*, *supra* note 160.

[166] *Id.*

[167] Memorandum from the Eur. Comm'n, Restoring Trust in EU-US Data Flows – Frequently Asked Questions (Nov. 17, 2013), *available at* http://europa.eu/rapid/press-release_MEMO-13-1059_en.htm.

create an internal data protection system that allows it to transfer data within the enterprise and among its partners and subsidiaries.[169] In order to use BCRs, the enterprise must have the rules approved by a DPA within a Member State.[170] Once it is approved in one Member State, the BCRs are forwarded to other DPAs in other Member States for approval.[171] The entire process is extremely complex, complicated, confusing, and time-consuming.[172]

BCRs can be an effective compliance tool, but they are very often costly to implement which would bar many small to medium size enterprises from using them.[173] There are only a few enterprises that possess the necessary income required to hire specialized law firms that can actually create and develop BCRs that are effective; enterprises such as General Electric, Hewlett Packard, Intel, Michelin, and Shell do not represent the entire international commerce community.[174] Also, BCRs only apply to transfers of data within one corporate group.[175] So, for non-EU firms to actually use them, they would need to establish an office within the EU.[176]

Almost all non-EU enterprises request the continued ability to use these compliance tools in order to comply with the GDPR, but the most recent amended version of the GDPR limits the

---

[168] Mittman, *supra* note 147.

[169] *Id.*

[170] *Id.*

[171] *Id.*

[172] *Id.*

[173] ECIPE, *supra* note 10, at 9.

[174] *See* K. Royal, *The ABCs of BCRs*, IAPP (May 13, 2013), https://www.privacyassociation.org/privacy_perspectives/post/the_abcs_of_bcrs; *see also List of Companies for Which the EU BCR Cooperation Procedure is Closed,* EUROPEAN COMMISSION, http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm (last updated Feb. 20, 2015).

[175] Restoring Trust in EU-US Data Flows – Frequently Asked Questions, *supra* note 167.

[176] *Id.*

use of compliance tools.[177] The GDPR acknowledges and recognizes only BCRs as a tool to transfer data across borders into states outside of the European Economic Area ("EEA").[178] To require such strict data protection requirements and then allow only one form of compliance for non-EU enterprises creates a death grip on international commerce and stifles the international flow of data.

IV. GDPR'S EFFECT ON NON-EU ENTERPRISES

The GDPR will have the greatest effect on two major democratic powers: The United States and India.[179] Together, the European Union and the United States account for half of the world's GDP and 2.4 trillion EUR in bilateral investments.[180] The value of EU-India trade in 2011 was 79.9 billion EUR and India is one of the most prominent data processing destinations.[181] Other major trading partners affected by the GDPR would include Japan, Singapore, and Korea.[182] These countries all have privacy legislation that protects personal data, but the EU does not *recognize* them as countries with adequate safeguards like the ones created with the GDPR.[183]

---

[177] *See Proposed GDPR*, *supra* note 4.

[178] *Radical Changes to European Data Protection Legislation*, *supra* note 54.

[179] ECIPE, *supra* note 10.

[180] *Id.*

[181] *Countries and Regions: India*, EUR. COMM'N, http://ec.europa.eu/trade/policy/countries-and-regions/countries/india/ (last visited Apr. 2, 2015).

[182] ECIPE, *supra* note 10, at 8.

[183] *Id.*

For example, American data protection has a foundation based upon the Fourth Amendment of the Constitution and its protection from illegal search and seizure.[184] Instead of one general and uniform law across the states, data protection in America is accomplished using a patchwork of legislation, similar to the EU's current patchwork of laws stemming from the Data Protection Directive. [185] The United States uses privacy laws and regulatory compliance laws to achieve its goal of protecting citizens' data and applies different laws to different situations.[186] Comparatively, the American patchwork still is not as in depth as its European counterpart, but it does protect personal data.[187]

The United States has established a number of laws that each state must adhere to, such as the Federal Trade Commission Act ("FTC Act"), the Financial Services Modernization Act ("Gramm-Leach-Bliley Act"), the Health Insurance Portability and Accountability Act ("HIPAA"), the HIPAA Omnibus Rule, Security Breach Notification Rule, the Fair Credit Reporting Act, Fair and Accurate Credit Transaction, the Controlling of Non-Solicited Pornography and Marketing Act ("CAN-SPAM Act"), the Telephone Consumer Protection Act, the Electronic Communications Privacy Act, and the Computer Fraud and Abuse Act.[188]

---

[184] *Five Myths Regarding Privacy and Law Enforcement Access to Personal Information in the European Union and the United States,* U.S. DEP'T. OF STATE, http://photos.state.gov/libraries/useu/231771/PDFs/Five%20Myths%20Regarding%20Privacy%20and%20Law%20Enforcement_October%209_2012_pdf.pdf (last visited Apr. 2, 2015).

[185] Ieuan Jolly, *Data Protection in United States: Overview*, LOEB & LOEB LLP (July 1, 2013), http://uk.practicallaw.com/6-502-0467#null; Cecile Martin, *Navigating the Patchwork: When is European Data Privacy Law Applicable to US Companies?*, PROSKAUER (Apr. 17, 2013), http://privacylaw.proskauer.com/2013/04/articles/online-privacy/navigating-the-patchwork-when-is-european-data-privacy-law-applicable-to-us-companies/.

[186] *United States Privacy Laws*, INFO. SHIELD, http://www.informationshield.com/usprivacylaws.html (last visited Apr. 2, 2015); *Regulatory Compliance: Security Policy and Organization*, INFO. SHIELD, http://www.informationshield.com/compliance.html (last visited Apr. 2, 2015).

[187] Richard Adhikari, *America's Perilous Patchwork of Privacy Laws*, TECHNEWSWORLD (Mar. 18, 2011), http://www.technewsworld.com/story/72092.html.

Additionally, many states have their own privacy laws, especially states like California, that attempt to patch the holes created by the federal laws.[189] These laws in combination with compliance tools like Safe Harbor should satisfy EU data protection standards adequately enough to allow data to flow transborder into the U.S.

V. THE EU-US DATA PROTECTION CONTROVERSY

The EU Institutions are unsatisfied with the United States' approach to data protection and after the most recent surveillance scandal, the Commission has released a list of thirteen data protection recommendations for the U.S.[190] These thirteen recommendations incorporate the data protection concepts of transparency, redress, enforcement, and access.[191]

The transparency and redress ideas help to protect EU citizens directly. The transparency concept requires the U.S. to ensure their enterprises publically disclose privacy policies, which include a link to the Department of Commerce Safe Harbor website, publish privacy conditions of contracts enterprises have with subcontractors, and clearly flag all enterprises that are not a part of Safe Harbor on the Department of Commerce Safe Harbor website.[192] The redress concept requires the U.S. to ensure its enterprises have links to alternative dispute resolution ("ADR") providers on their website that are readily available and affordable.[193] The Department

---

[188] Jolly, *supra* note 185.

[189] *United States Privacy Laws*, *supra* note 186; Jolly, *supra* note 185.

[190] Restoring Trust in EU-US Data Flows – Frequently Asked Questions, *supra* note 167.

[191] *Id.*

[192] *Id.*

[193] *Id.*

of Commerce must monitor the ADR providers to ensure they are abiding by rules that are set forth.[194]

The enforcement and access ideas help to police U.S. enterprises. The enforcement concept requires the U.S. to perform investigations to ensure enterprises are complying with Safe Harbor. [195] If an enterprise is found to be non-compliant a further specific investigation should be held one year later to ensure corrective measures were put in place.[196] The U.S. must also investigate any false claims of Safe Harbor compliance. When the Department of Commerce has doubts to an enterprise's compliance with any EU data protection standard, it must inform the appropriate EU DPA.[197] The access concept requires U.S. authorities to review privacy policies to ensure that exceptions to data protection standards for national security, public interest, and law enforcement are necessary and appropriate.[198]

The EU Institutions dispute the validity and self-regulatory nature of Safe Harbor and the actual reach of the FTC's enforcement powers.[199] However, just as a DPA would oversee and sanction an enterprise in the EU, the FTC has also served as a sufficient and aggressive enforcer of data protection in the United States. For instance, one major argument against Safe Harbor is that a number of companies have claimed to be Safe Harbor certified when in actuality they were not.[200] The FTC has charged twelve different enterprises for falsely asserting compliance with

---

[194] *Id.*

[195] Restoring Trust in EU-US Data Flows – Frequently Asked Questions, *supra* note 167.

[196] *Id.*

[197] *Id.*

[198] *Id.*

[199] Aplin, *supra* note 159.

Safe Harbor.[201] All twelve enterprises were previously certified under Safe Harbor but their certifications had lapsed.[202] The enterprises involved National Football League teams, as well as a major communications company.[203] The firms involved all had websites stating that they were current with their Safe Harbor compliance and therefore were all charged with making false claims.[204] Even though none of the charges alleged any substantial violations of the Safe Harbor data protection principles, the FTC has made a point to show that it respects EU data protection guidelines.[205]

The other main issue that the EU Institutions have with the U.S. in regards to data protection is that the EU citizen has no power to seek redress.[206] In the U.S., non-citizens seek judicial redress for wrongs committed against them in federal court.[207] Federal Courts hear cases involving laws and treaties of the U.S,[208] as well as hear cases involving subjects and citizens of foreign states.[209] People in the EU could file claims and seek damages against American

---

[200] *Is The Safe Harbor Program Still Safe?*, ALLEN & OVERY (Oct. 2, 2013), https://www.aohub.com/aoos/viewContent.action?key=Ec8teaJ9VaqLGpSUqS%2FLgl7eOOGbnAEFKCLORG72fHz0%2BNbpi2jDfaB8lgiEyY1JAvAvaah9lF21%0D%0ACiGG39vtfQ%3D%3D&nav=FRbANEucS95NMLRN47z%2BeeOgEFCt8EGQ%2FHLCIrtYuIY%3D&uid=frsvcLdHNrI%3D&popup=HxapDW%2FMKd4%3D&freersslink=true.

[201] Aplin, *supra* note 159.

[202] *Id.*

[203] *Id.*

[204] *Id.*

[205] *Id.*

[206] Restoring Trust in EU-US Data Flows – Frequently Asked Questions, *supra* note 167.

[207] *Jurisdiction Of The Federal Courts*, U.S. CTS., http://www.uscourts.gov/FederalCourts/UnderstandingtheFederalCourts/Jurisdiction.aspx (last visited Apr. 2, 2015).

[208] *Id.*

[209] 28 U.S.C. § 1332(a)(2) (2014).

enterprises that violate U.S. laws that protect personal data.[210] The major issue is that U.S. laws do not protect EU citizens.

For example, the 1974 Privacy Act only protects U.S. citizens and permanent residents.[211] This means that even if an American enterprise violates the 1974 Privacy Act by illegally transferring an EU citizens personal data, the EU citizen will not be able to seek judicial redress in the American court system because they were not protected under the law. This is a valid concern but how can the EU expect the U.S., or any other third country for that matter, to create legislation that protects or controls citizens that are not under their jurisdiction?

VI. THE RIGHT TO CHOOSE – THE GDPR'S MISSING LINK

Until new data protection laws are ratified within the U.S. and other third countries, the EU Institutions should allow Data Subjects to consent as to whether or not they would allow a non-EU enterprise to process their data knowing that once it crosses the EU borders, it is not under the jurisdiction of the GDPR. This allows the Data Subject the "Right to Choose" how and where they want their personal data processed. Essentially, the GDPR's all-encompassing and widespread ban actually hinders the Data Subjects' rights. If the Data Subject wants his personal data to be processed by a non-EU firm, then that should be the Data Subject's uninhibited choice. This ability to consent truly allows uninhibited transborder data flow.

EU Model Clauses and BCRs are simply contractual statements to which enterprises agree. There is no magical power behind them. In the same respect, Safe Harbor is another form

---

[210] U.S. CTS., *supra* note 207.

[211] Restoring Trust in EU-US Data Flows – Frequently Asked Questions, *supra* note 167.

of contractual compliance. When enterprises utilize these compliance tools, they are simply entering into contracts with each other to be responsible for the safe processing and storing of data. If the EU Institutions are not willing to accept that other States can provide proper safeguards to personal data and enforce them amongst their respective enterprises, then the people in the EU should be allowed to decide whether or not they want to do business with enterprises outside of the EEA.

The GDPR has entire sections dedicated to clear consent and therefore should extend consent to include the "Right to Choose." International trade and commerce depends on transborder data flow and each person should have the "Right to Choose" how their own personal data will be processed. If the Data Subject does not want to have their data processed outside of the EEA, then it can refrain from giving consent or withdraw consent when notified that the data will be traveling outside of the EEA zone. The Data Subject has a number of rights and the "Right to Choose" is their most important one in regards to personal data protection.

CONCLUSION

The EU Institutions' push to protect the individuals fundamental right of privacy and personal data protection is understandable. There is a definite need for legislation that will allow a Data Subject the ability to control the use of his personal data. But, broad sweeping legislation is not the answer especially when the legislation attempts to force jurisdiction over other sovereign nations and their enterprises. In fact, the GDPR pushes the boundaries of the EU's international law without allowing proper compliance tools that allow enterprises to conform. The GDPR's attempt to use a "one size fits all" resolution to a worldwide problem will not work.

The GDPR must be further amended to allow a more widespread method of compliance or allow the Data Subject to make their own decisions on the protections of their own personal data.

SYRACUSE JOURNAL OF SCIENCE & TECHNOLOGY LAW

VOLUME 31 2014-2015 ARTICLE 9, PAGE 251

THE NEW KINSHIP: CONSTRUCTING DONOR-CONCEIVED FAMILIES

Ashley Jacoby[1]

Citation: NAOMI CAHN, THE NEW KINSHIP: CONSTRUCTING DONOR-CONCEIVED FAMILIES (2013).

Relevant Legal and Academic Areas: Family Law, Constitutional Law, Privacy Law, Assisted Reproductive Technology, Biology

Summary: *The New Kinship: Constructing Donor-Conceived Families* explores how families are made and bonds are formed between families in light of the advances in the field of reproductive technology. Author Naomi Cahn, an expert on reproductive technology and law, gives an overview of the world shared by parents, children, and gamete donors who turn to assisted reproductive technology to create their own families. The book examines how the law has developed in the field, and advocates that increased regulation is necessary based on numerous social, economic, and legal grounds.

INTRODUCTION

In *The New Kinship: Constructing Donor Conceived Families*, author Naomi Cahn examines how families and relationships form when individuals utilize assisted reproductive technology ("ART") to conceive and bear children.[2] Cahn proposes that *The New Kinship* serves three purposes: firstly, it explores how emotional connections are created and develop within families who opt to use donor gametes, and documents these evolving relationships; secondly, it offers a legal foundation for promoting the development of these communities, and argues that current law should not be primarily focused on medicine, technology, and commodification, but rather family and constitutional law; thirdly, *The New Kinship* illustrates how donor families

[1] Syracuse University College of Law, Juris Doctorate expected 2015.

[2] NAOMI CAHN, THE NEW KINSHIP: CONSTRUCTING DONOR-CONCEIVED FAMILIES ix (2013).

simultaneously reinforce and complicate the meaning of family, thereby offering an opportunity to reconsider the meaning of family generally.[3]

In seeking to offer an in-depth look at how "donor families" both support and confuse the social, cultural, economic, and legal meaning of family, Cahn offers a chronological and thematic exploration of the donor world.[4] Consequently, this review will begin by examining the basic meaning of family and outlining the composition of the donor world. The second section of the review will address the questions of "who" searches for donor-based relationships, and "why." The third section examines the law's approach to, and relationship with, donor-conceived families. The last section discusses Cahn's proposals for legal reform in this emerging area of law. The review will conclude by addressing the broader implications and benefits of allowing for the expansive construction and conception of the meaning of family.[5]

I. THE MEANING OF FAMILY AND THE TERRAIN OF THE DONOR WORLD

In the first section of *New Kinship*, Cahn provides a brief overview of the donor-gamete world.[6] Cahn argues that because of the stigma attached to infertility and impotency, and the value given to sharing genes with family, it is important to understand who drives the multi-million dollar reproductive technology industry.[7]

---

[3] *Id.* at 3.

[4] CAHN, *supra* note 2, at 5.

[5] *Id.* at 5-6.

[6] *Id.* at 14.

[7] *Id.* at 13.

A. People in the Donor World

Reproductive technology is for many people—gay, lesbian, single, medically infertile, or partnered with someone medically infertile—the only chance to experience childbirth.[8] Cahn argues that the growth and development of the fertility industry, and an evolving understanding of the family structure, has created a new reproductive culture reflective of a postindustrial economy.[9] Specifically, the postponement of childbearing, and the growing acceptance of non-marital cohabitation and same-sex couples has drastically increased the number of people using ART within the last few decades.[10] Although income has not seemed to affect an individual's initial decision to seek ART services, women with higher sources of income have a greater chance of pursuing more intensive forms of treatment.[11] Furthermore, access to health insurance influences an individual's decision to pursue different treatment options.[12]

Despite the growing acceptance of using ART to conceive, both men and women are significantly more likely to view using donor sperm negatively.[13] Researchers have indicated this widespread perception can be attributed to a number of factors. For instance, one study in 2010 deduced that both men and women believe that using donor sperm will create marital conflict, is more likely to result in social judgment and criticism of parenting skills, and is less likely to result in a satisfying childbearing experience.[14] Other studies have "speculated that 'while many assume a mother would love a child regardless of genetic relatedness, a father does not generate

[8] *Id.* at 14.

[9] CAHN, *supra* note 2, at 15.

[10] *Id.* at 14.

[11] *Id.* at 16.

[12] *Id*. at 16.

[13] *Id.* at 17.

[14] CAHN, *supra* note 2, at 17.

similar feelings of selflessness . . . and in patriarchal society where children inherit the father's name, maternal relatedness is less important.'"[15]

Thus, gendered social norms and the development of intracytoplasmic sperm injection (ICSI), which has significantly decreased the need to utilize donor sperm, indicate that the use of donor eggs is more socially acceptable.[16] However, donor eggs are typically available only under two circumstances; firstly, when women already undergoing an in vitro fertilization (IVF) cycle agree to provide their eggs to other women in exchange for a reduced IVF fee; secondly, when women outside of a fertility clinic are recruited to donate their eggs.[17] Furthermore, until recently there has been limited access to egg brokers, and the use of donor eggs still necessitates recipients utilize a fertility clinic and a cycle of IVF.[18] Contrastingly, a vile of sperm costs less than $350, can be shipped from any one of 150 sperm banks throughout the United States, and can be implanted in the comfort of a woman's home.[19] Consequently, the general conclusion in the donor world and society generally is that "egg donors are altruists" while "sperm donors are in it for the money."[20]

To police this evolving industry, states and self-regulating professional organizations have attempted to control the safety and quality of the donor world.[21] States are, in general, responsible for overseeing health professionals and ART procedures.[22] However, the federal

[15] *Id.* at 17.

[16] *Id.* at 18.

[17] *Id.* at 21.

[18] *Id.* at 19.

[19] CAHN, *supra* note 2, at 19.

[20] *Id.* at 28.

[21] *Id.* at 23.

government has recently become more involved in monitoring fertility clinic success rates and regulating clinical laboratory services, drugs, and medical devices used in IVF treatments.[23] Specifically, the federal government asserted its interest in regulating the fertility industry market and providing safeguarding against deceptive clinic practices in 1992 when Congress passed the Fertility Clinic Success Rate and Certification Act.[24] Nevertheless, Congress has been extremely deferential to the ART industry.[25] For example, FDA guidelines do not control how ART practices are conducted, but rather regulate the collection, processing, storage, and distribution of human gametes "as the 'articles' of ART."[26] The ART industry has also opposed further regulation, and consistently relied on self-regulation, voluntary and ethical standards, and consumer need to drive the industry forward.[27]

Consequently, in the United States, future parents, donors, medical professionals, and the government share an interest in the multi-billion dollar a year business of producing families.[28] However, these parties often have varying incentives for driving the industry into the future.[29]

B. The Meaning of Family in a Changing World

The New Kinship maintains that the goal of participating in the donor world is "to have a child in order to create, complete, or expand one's family."[30] Cahn also maintains that the

---

[22] *Id.* at 23.

[23] *Id.* at 23.

[24] CAHN, *supra* note 2, at 23.

[25] *Id.* at 24.

[26] *Id.* at 24.

[27] *Id.* at 27.

[28] *Id.* at 27.

[29] CAHN, *supra* note 2, at 30.

government, donors, clinics, and parents-to-be are "stakeholders" in the ART industry's endeavor to create each individually constructed vision of "family."[31] However, Cahn also argues that these parties challenge our understanding of that word,[32] and consequently, donor-conceived families and the communities they create illuminate the need to address the modern conception of "family."[33]

As a preliminary matter, *The New Kinship* identifies two different kinds of "donor families." The first kind, formed with the assistance of donor gametes, is a "donor-conceived family."[34] A single parent, or couple, chooses to create a donor-conceived family by using donor eggs, sperm, or embryos to create a child.[35] This method results in a child, but impacts the ways in which partners understand each other, their roles as parents, and their own emotional connection.[36] As a result, using third-party gametes to produce a donor-conceived family produces both parent and child.[37]

The second type, "donor-conceived family communities," or "donor kin families or networks," accounts for two different sets of relationships based on genetics.[38] The first relationship is between the donor and any offspring produced, and the second relationship is

---

[30] *Id.* at 31.

[31] *Id.* at 30.

[32] *Id.* at 30.

[33] *Id.* at 33.

[34] CAHN, *supra* note 2, at 2.

[35] *Id.* at 2.

[36] *Id.* at 2.

[37] *Id.* at 2.

[38] *Id.* at 2.

among *all* of the children created by a particular donor's gametes and their individual families.[39] Donor conceived family communities can potentially include tens or even hundreds of people, who often think of themselves as kin despite the fact that their relationships are based on a parent's unintentional choice to use a common donor.[40]

Thus, donor families fundamentally challenge the societal understanding of family as based on blood and genes.[41] Specifically, ART runs the risk of "undermining the traditional family" because it can give children to single parents, parents of the same sex, and heterosexual couples without sexual intercourse; notions of motherhood and fatherhood are seemingly ambiguous.[42]

However, some social scientists have argued that because ART focuses on the science of reproduction, it actually supports the conventional understanding of family as based on biological bonds.[43] For example, some scientists maintain that the choice to use donor gametes and the search for genetically related family members replicates a family dynamic that would have existed notwithstanding an individual's infertility.[44] Therefore, ART may be traditional in the sense that it relies on the concept of a biological relationship and the creation of a child to form a family.[45]

---

[39] CAHN, *supra* note 2, at 2.

[40] *Id.* at 2.

[41] *Id.* at 32.

[42] *Id.* at 33.

[43] *Id.* at 33.

[44] CAHN, *supra* note 2, at 33.

[45] *Id.* at 33.

Like the societal understanding of family, the legal interpretation is also conflicted.[46] However, the definition of family within the meaning of the law has historically implicated *status*.[47] For example, a child can inherit from a parent because the law bestows a relational status between them.[48] Historically, relational status has depended on biology or adoption.[49] However, in the more recent past, the law has been willing to evaluate relational status based on a person's functioning as a parent by providing care for a child.[50] The expansion and evolution of the donor world thus exemplifies how a biological relationship is insufficient to confer the legal status the meaning of family otherwise provides.[51]

The unique economic nature and commerciality of the donor world also complicates the question of how donor families affect the meaning of family.[52] Cahn argues that because donors sell their bodily parts to individuals expecting to pay, that commercial transaction actually implies that a family relationship has been created.[53] While some scholars have argued that commercializing the "miracle of the passing on of human life" is unethical, others, like Cahn, have argued that commodifying gametes reinforces and fosters the creation and meaning of family, and also accurately reflects the economic value of work performed.[54] Consequently, *The*

[46] *Id.* at 33.

[47] *Id.* at 35.

[48] *Id.* at 35.

[49] CAHN, *supra* note 2, at 35.

[50] *Id.* at 35.

[51] *Id.* at 35 (explaining that children conceived after the death of a biological parent with the assistance of ART may not be recognized as the legal child because the law in certain instances treats the gametes of a dead spouse in the same way as those of an anonymous donor).

[52] CAHN, *supra* note 2, at 39.

[53] *Id.* at 39.

[54] *Id.* at 42.

New Kinship takes the position that the relevant question must necessarily be what aspect of gamete donation to commodify, and how this impacts the definition of family: "[t]he movement to understand market relationships as more than economically based, as social, helps us, simultaneously, in understanding that social relationships, such as the family, are not just socially based but are economic as well."[55]

II. CREATING DONOR-CONCEIVED FAMILIES AND COMMUNITIES

A. Creating Families

When families-to-be enter the donor world, they enter with the primary goal of creating a life. However, most people wish to bear a child that is genetically related to at least one partner, or at a minimum, has "good genes."[56] Thus, members of the donor world begin to create their own sense of family in a "cultural context where biogenetic relationships are central, almost 'mystical.'"[57] In other words, genes matter.

To illustrate her argument that genes play a critical role in creating a family, Cahn focuses on the recently publicized controversy over "designer babies."[58] This ethical microcosm—choosing specific attributes to give to a child—highlights how an emphasis on genes in the donor world has confused the understanding of family. On the one hand, selecting gametes for "brains, brawn, or deafness" raises the serious ethical issues of selective breeding and eugenics.[59] On the other, the decision to use gametes shows that ART services are in fact

---

[55] *Id.* at 44 – 45.

[56] *Id.* at 49.

[57] CAHN, *supra* note 2, at 49.

[58] *Id.* at 52.

producing family and kinship, and that the actual process of choosing a donor creates bonds between parents, children, donors, donor-conceived family members, and between families who have used the same donor.[60] Thus, despite the fact that using donor gametes necessitates that a third party become part of the choice to reproduce, careful selection of the gametes can enable parents to minimize the role the donor played in creating their family.[61] This act, in turn, can help parents feel connected to and in control of their reproduction, as well as their child's future, thereby assisting in the creation of a family.[62]

B. Creating Communities Across Families

The perception that genetically related family trumps any other version of family is deeply engrained in American society. For this reason, disclosure of a child's genetic origins remains a highly volatile issue in the donor world; while disclosure can allow children and their legal parents to develop *interfamilial* bonds and provide a foundation for gaining insight into the origins of their family, many parents opt to keep their use of donor gametes a secret for fear of weakening *intrafamilial* bonds.[63]

However, many parents of children conceived with ART do make an informed decision to tell their children how the children were conceived, and studies have illustrated that both parents and children benefit from openly discussing the subject.[64] The results of such disclosure,

---

[59] *Id.* at 53.

[60] *Id.*

[61] *Id.* at 54.

[62] CAHN, *supra* note 2, at 54.

[63] *Id.* at 62 (emphasis added).

[64] CAHN, *supra* note 2, at 68 – 69.

moreover, exemplify how donor-conceived family communities expand the societal notion of family, and challenge the structure of the "nuclear heterosexual family."[65] Without the expectation of finding shared cultural, religious, or social heritage, many donor-conceived children and their parents seek out their donor parent(s) and siblings in order to satisfy their personal curiosities and desire to create a larger family.[66] Furthermore, donors also elect to abandon their anonymity in order to learn what became of their donation, and will sometimes even pursue a relationship with their biological offspring.[67] Nonetheless, while children, parents, and donors may seek out a different type of relationship or choose to form a greater emotional connection with one another, the legal framework that might support the growing web of donor-conceived family communities and their respective networks is minimal at best.[68]

III. THE LAW AND DONOR FAMILIES

Given that ART and the donor world raises a multitude of legal issues, it is surprising just how little guidance the law provides to members of the developing donor-created kin networks. *The New Kinship* maintains that currently the law minimally regulates donor family relationships, just as it minimally regulates other areas of reproductive technology, and that the absence of a more comprehensive framework is deeply problematic for United States policy.[69]

---

[65] *Id.* at 73.

[66] *Id.* at 73.

[67] *Id.* at 86. For instance, Mike Rubino, known as Donor 929 at the California Cryobank, determined to learn what happened to his sperm donation. *Id.* Through the Donor Sibling registry (DSR), Rubino learned Racael McGhee had given birth to two children conceived using his donation. *Id.* The biological parents and their two children thereafter spent time together learning about each other. *Id.*

[68] CAHN, *supra* note 2, at 87.

[69] *Id.* at 92.

While each state has its own unique method of determining who the legal parents of children conceived with ART are, the law relies primarily on contract, marriage, biology, intent, or a "best interests of the child" standard to make that legal determination.[70] Still, perhaps the strongest factor in determining parenthood is based on the historically rooted marital presumption; dating back to the 1700s, the marital presumption dictated that a married man and woman were the parents of a child born into the marriage.[71] Today, the presumption remains entrenched in state law throughout the nation, and applies to both heterosexual and homosexual couples (where homosexual marriage is recognized).[72] The judicial rationale for preserving this presumption, which again reflects the social concept of what it means to have a family, is that states have interests in preserving the "sanctity of marriage" and that a child be raised in a functionally stable home.[73]

However, with the passage of the Uniform Parentage Act (UPA) in 1973, Congress attempted to create a standardized law that would produce consistent parental determinations regardless of a child's place of birth.[74] The UPA specifically contemplated donor-conceived children, and provided that if a married woman was inseminated, then her husband would become the legal father of any resulting child, so long as the husband gave consent to the insemination, and a licensed physician supervised the procedure.[75] Because the UPA did not

[70] *Id.* at 92.

[71] *Id.*

[72] *Id.* at 92.

[73] CAHN, *supra* note 2, at 93.

[74] *Id.* at 93.

[75] *Id.*

address a scenario in which an *unmarried* woman might conceive a child with the aid of ART, it could not bar single and lesbian women from entering the donor world on their own.[76]

Today, the UPA, revised in 2002, specifically contemplates the issues that might be raised with technological advances, including artificial insemination using donor gametes and the ability to freeze eggs and sperm.[77] The Act holds that neither an egg nor sperm donor is a child's legal parent if that child is not conceived through sexual intercourse, and states specifically that a male donor is not the father of a resulting child unless he signs a consent to paternity, or else lives with the child throughout the child's first two years of life and "holds out the child as his offspring".[78] While the revision has expanded the original Act to include unmarried couples and egg donors, it still does not account for same-sex couples and newer ART services.[79] A minority of states has adopted and currently follows the UPA.[80] The majority of states terminate the potential parental rights of unknown sperm donors, while only some terminate the rights of anonymous egg donors.[81]

The law on establishing parental rights when an individual or couple utilizes a known donor is in confusion throughout the states. A jurisdiction's individual determination as to the state of parents' and donors' legal rights reflects that jurisdiction's position on whether biology, marriage, or contract law should dictate the outcome of familial identity.[82] Furthermore, many states have not addressed the issues surrounding parenthood by ART for non-married couples,

[76] *Id.* at 94 (emphasis added).

[77] *Id.* at 94.

[78] CAHN, *supra* note 2, at 94.

[79] *Id.* at 95.

[80] *Id.* at 95.

[81] *Id.* at 95.

[82] *Id.* at 95.

egg donors, physician involvement, and known donors, while the remaining states have created a hodgepodge of case law often decided narrowly and that continues to fluctuate.[83]

Like the law establishing rights as between parents and children, the law determining sibling rights is also confused. In general, existing law does not clearly support rights as between siblings conceived with donor gametes, but a number of attorneys and individuals with a stake in a legal determination on the subject have made creative arguments in support of a basis for establishing siblings' rights.[84] For example, Supreme Court decisions have found a basis for protecting familial relationships, and via a Fourteenth Amendment Due Process Clause argument, sibling associational rights may fit within the jurisprudence.[85] Furthermore, the Supreme Court has found that the First Amendment protects the rights of siblings to remain in contact with each other.[86] Weighing against a sibling's interest and right to association is of course the parental desire and wish to prevent such communication.[87] Scholars and attorneys have made a number of policy arguments reasoning that the social importance of fostering sibling relationships necessitates ensuring sibling relationships remain intact.[88]

In conclusion, the disarray of law in this field indicates that state law supporting the development of new relationships between individuals who are genetically related through a common donor will likely not be strictly applied. *The New Kinship* maintains that this is the appropriate direction for the legal precedent to land; the law should "focus on the meaning of

[83] CAHN, *supra* note 2, at 95.

[84] *Id.* at 103.

[85] *Id. at* 104.

[86] *Id. at* 104.

[87] *Id.* at 104.

[88] CAHN, *supra* note 2, at 104.

family, not the technology and medicine that create the family members" because "recognizing connections among donor-conceived kin is as much about the meaning of family as it is about how to regulate families."[89]

IV. TO REGULATE OR NOT?

In contemplating the future of regulation for ART, Cahn argues that existing legal constructs should be expanded to recognize the importance of developing a framework that emphasizes family and personhood in the donor world.[90] Generally, Cahn cites identity issues and the complexity of the law as factors weighing in favor of regulation.[91] Furthermore, Cahn maintains that regulation is critical at two specific points.[92] Firstly, the law should elucidate the legal relationships among offspring, recipients, and donors.[93] Secondly, the law should foster connections between donor-conceived families sharing genes.[94] At its most fundamental level, Cahn writes, the ART industry is about creating families, and thus the industry framework needs to be reconsidered so that it is subject to laws that regulate people, and not things.[95]

Consequently, *The New Kinship* takes the position that a few distinct measures are necessary to ensure a workable legal model protects and regulates the donor world. Specifically, Cahn argues that states need to recognize written agreements between donors, recipients, and

---

[89] *Id.* at 105.

[90] *Id.* at 125.

[91] *Id.* at 129-31.

[92] *Id.* at 135.

[93] CAHN, *supra* note 2, at 135.

[94] *Id.* at 135.

[95] *Id.* at 136.

other families.[96] Furthermore, donor gametes should be subject to increased medical testing and scrutiny, with Legislatures requiring improved record keeping, more extensive counseling and disclosure to parents and donors, and limiting the number of children that may be born from a particular donor's gametes.[97]

Cahn does acknowledge that scholars and attorneys alike have propounded arguments against regulating the donor world and ART community.[98] However, to accept the arguments against regulating the industry, she maintains, would fail to recognize that the donor world consists of many different types of families, but families nonetheless.[99]

CONCLUSION

Much of the donor world remains uncharted.[100] *The New Kinship* proposes a paradigm shift toward regulating donor-conceived families and the communities they create so that they can more properly be understood as relational entities.[101] Cahn argues that while law currently exists that may be used as a background to develop these families, a new model is necessary in order to provide structure in the face of the challenges implicated by these expanding communities.[102] Although *The New Kinship* does not propound that donor family communities

[96] *Id.* at 150.

[97] *Id.* at 151.

[98] *See* CAHN, *supra* note 2, at 151.

[99] *See id.* at 162.

[100] *Id.* at 181.

[101] *Id.* at 181.

[102] *Id.* at 182.

need special treatment, Cahn concludes that only when a new model is produced as a result of such a paradigm shift can the diversity and pluralism of family forms be fully appreciated.[103]

[103] CAHN, *supra* note 2, at 182.