SAINT LOUIS UNIVERSITY LEGAL STUDIES JOURNAL

Special Edition: The Right to Privacy

Spring 2014

PROFILE OF THE GUEST EDITOR-IN-CHIEF

Morgan Hazelton is a member of the Political Science Department at Saint Louis University. She holds a law degree from the University of Texas at Austin and is a PhD Candidate in the Political Science department at Washington University in St. Louis. Prior to academia, she practiced law in Texas. In 2008, she was named the El Paso Outstanding Young Lawyer of the year. Her research and teaching interests encompass American political institutions, judicial politics, and quantitative methods with a focus on litigation and judicial impact and hierarchy. She has previously taught at the University of Texas in El Paso and Washington University in St. Louis. In 2011, she received a Dean's Award for Teaching Excellence at Washington University in St. Louis.

GUEST EDITOR-IN-CHIEF'S INTRODUCTION TO THE ISSUE

This journal represents the collective efforts of students, staff, faculty, and attorneys in the Saint Louis University community; like the Pre-Law program at Saint Louis University itself, this journal is the product of interdisciplinary and interprofessional exchanges, and represents a fine example of what such exchanges have to offer to society. Saint Louis University is a vibrant and collegial environment in which students can undertake such projects with the full support of faculty, staff, and volunteers. The mentors were invaluable assets in the creation of this journal.

For this third issue of the Saint Louis University Legal Studies Journal, our contributors grapple with important and complex issues regarding privacy. In light of the advent of social media and revelations regarding governmental surveillance highlight, few issues are as important as privacy to understanding the relationship among the individual, society, and government. Privacy plays a key role in many essential areas of jurisprudence, both in the United States and internationally. It is a bedrock concept in both criminal and civil law, with deep implications for the rights of the individual with regard to the government as well as businesses and other citizens.

The concept of privacy does not lend itself to easy definition: there are competing definitions based on ideas about seclusion and the right to control information about oneself reveal, among others. Furthermore, the debate over the definition of privacy is deeply influenced by the changing nature of how information is collected and shared and the expectations that citizens have with regards to privacy. These articles span a broad range of issues related to privacy and reveal the complexities of the concept.

Two of the articles in this issue pertain to issues of privacy in the digital age in terms of control over information communicated via the internet. First, Michelle Palka considers issues of privacy online for individuals in the United States. Specifically, she considers what expectations of privacy an individual can reasonable hold with regards to commercial and governmental access to data. She offers a balanced analysis that considers both the safety benefits of access by the government and potential economic benefits of access by business against the costs to individuals and their privacy. She ultimately concludes that the competing interests regarding information are such that a savvy user should have rather modest expectations regarding the private nature of their activity on the internet.

Ashley Johann compares governmental responses in the United States and Germany to Facebook policies and activities to compare American and European approaches to legislating regarding privacy in regards to data security and information control. Her article highlights the difficulties faced by companies in light of the lack of an international standard and offers possible responses to the inconsistent standards. Her analysis illustrates the extent to which the United States is moving towards a more European conception of individual rights with regard to notice and consent regarding personal information. At the same, she aptly points out that the privacy approach in the United States ignores many potential aspects that the European approach address, such as rights to access and corrections.

Caitlan Grombka-Murphy also considers the relationship between new technologies and privacy, but from the perspective of criminal investigation and prosecution. She provides a detailed criticism of the 2013 Supreme Court decision in *Maryland v. King*, in which the Supreme Court ruled (5 to 4) that law enforcement officers can take and test DNA samples from arrestees suspected of committing serious offenses, as they do with fingerprints. Grombka-Murphy offers several sophisticated arguments regarding the extent to which allowing such testing represents a broad and unprecedented threat to privacy and civil rights. First, such samples are not merely used for purposes of identification, but rather for discovery and investigation regarding unsolved cases; she asserts that allowing for such warrantless activities is far outside of prior understandings of the Constitution. Also, DNA contains a wealth of potential information regarding individuals and their biological relatives that extends beyond what is needed for law enforcement and this information is not properly safeguarded. Finally, Grombka-Murphy asserts that decision will result in an overburdening of the DNA database that may ultimately hinder law the justice system.

A second-time contributor, Petina Benigno takes on the best means of interpreting the Fourth Amendment based on asserts that a clear rule regarding the Fourth Amendment based on economic analysis would provide for ex ante analyses regarding searches that would maximize societal and individual benefits. With the goal of reducing the number of unconstitutional searches that occur, she analyzes the nature of rules and standards within the framework of ex ante and ex post review. She promotes a cost-benefit analysis develop my Craig Lerner, based Learned Hand's formula from tort law, as a rule that would shift the focus to ex ante consideration by requiring the balancing and societal and economic costs against individual rights.

In his article, Jesse Doggendorf offers a different approach to privacy. Specifically, he considers the concept of privacy as a vehicle for the expansion of civil rights. His work stands at the intersection of philosophy, law, and activism as he considers the role of a Lockean ideal of privacy in advancing LGBT rights via Supreme Court jurisprudence. Doggendorf skillfully considers the arguments for and against asserting privacy as a means for recognizing additional rights for members of the LGBT community, including alternative the alternative framework of liberty. As part of this analysis he engages major Supreme Court precedents regarding the legal treatment of homosexuals and traces how the Court treats arguments of privacy that are inherently Lockean with the most favor.

I know I speak for all of the advisors and mentors when I say that one of the most rewarding aspects of working with students is watching them become scholars themselves and produce outstanding work such as you see in this journal. These authors are students who go above and beyond to engage the world around them. I would like to specially thank Janet O'Halloran and Joyce LaFontain for all of their hard work in putting this journal and issue together.

Professor Morgan Hazelton
Guest Editor-In-Chief
Saint Louis University Legal Studies Journal

Special Edition: The Right to Privacy

SAINT LOUIS UNIVERSITY LEGAL STUDIES JOURNAL

Vol. 3, No.1 Spring 2014

Privacy Expectations by Internet Users: Does Such a Thing Exist Anymore?

Michelle Palka

With the average American spending over five hours a day on non-voice mobile activities such as browsing the internet on their phones or tablets and searching through YouTube, the use of the internet has changed drastically from its original work-only environment.[1] The internet has also considerably transformed the way people communicate with each other, whether it be with someone across the world or simply down the street. With more opportunities for sharing information, research, sudden breaking news, and opinions, this has also raised the issue of how much privacy does one actually have once they open their browser. As technology continues to progress, the law has not kept pace with provisions that protect both internet users and companies.

One of the very first laws regarding internet privacy, passed in 1986, was known as the Electronic Privacy Communications Act (ECPA).[2] In the historical context, technology was just beginning to boom in the mid-eighties when Congress decided to pass the ECPA to extend government restrictions on wiretaps from telephone calls to include transmissions of electronic data by computer. Most would agree this is one of the first and most influential bills that began the long-standing dispute over the privacy of internet users. A more up-to-date version of the ECPA is the 2009 law that regulates software cookies and other unique digital markers which identify consumers that visit a certain web site and deliver ads which are tailored to the person's

[1] Adam Cohen, *Internet Privacy: A New Bill Finally Offers Protections,* TIME (April 30, 2013), http://ideas.time.com/2013/04/30/internet-privacy-a-new-bill-finally-offers-protections/.
[2] *Electronic Communications Privacy Act,* EPIC.ORG, http://epic.org/privacy/ecpa/ (last visited May, 15, 2014).

interests.[3] Throughout the years as technology has rapidly advanced and younger individuals are using the internet, there are many supporters of internet users being tracked.

National Security is a concern for every country and with more people having access to the internet, the world has slowly begun to shrink. Because of this, the government contends surveillance of American citizens is necessary for the benefit and safety of the entire society. By searching for key words, government Intel agents are confident they can ensure the safety of the country by finding those who are plotting dangerous attacks on the nation. This sparks the question of what role the government should play in monitoring people's behaviors and whether or not the government is overstepping their boundaries. The majority of people may agree that if the government is only looking for isolated cases of dangerous behaviors, then tracking everyone's data may be a small price to pay. Conversely, the National Security Agency (NSA)[4] has been under fire recently after tracking phone calls of ordinary American citizens and spying on international calls, text messages and emails for no apparent reason or suspicion of illegal activities. The NSA cited two laws passed by Congress in their defense: The Patriot Act and the FISA Amendments Act (FAA). The Patriot Act was introduced and passed under President George W. Bush after the 9/11 terrorist attacks and extended by President Barack Obama.[5] The purpose of the act is to allow for wiretaps, searches of business records and surveillance of individuals who are suspected of being involved with terrorist groups. The FAA allows for the monitoring of electronic communications that foreigners have abroad by the U.S. government.[6]

---

[3] Kevin J. O'Brien, *Setting Boundaries for Internet Privacy*, THE NEW YORK TIMES (Sept. 18, 2011), http://www.nytimes.com/2011/09/19/technology/internet/setting-boundaries-for-internet-privacy.html?pagewanted=all&_r=0.

[4] *About NSA*, NATIONAL SECURITY AGENCY, http://www.nsa.gov/about/index.shtml (last visited May 15, 2014).

[5] *The USA PATRIOT Act: Preserving Life and Liberty,* JUSTICE.ORG, http://www.justice.gov/archive/ll/highlights.htm (last visited May 15, 2014).

[6] ACLU, *Surveillance Under the FISA Amendments Act*, ACLU.ORG, https://www.aclu.org/time-rein-surveillance-state-0 (last visited May 15, 2014).

While I feel that it is necessary that the government do what they can in order to protect American citizens and prevent a tragedy such as 9/11 from reoccurring, tracking every American's data usage and reading private text message exchanges of people with no criminal records is overstepping the boundary. The two previously mentioned acts are intended to specifically target illegal and unusual activities that pose a harm to society. Reading private communication exchanges between citizens seems to be a stretch and an unreasonable use of government resources. With the few exceptions of public safety, terrorism, having probable cause, the right to privacy is protected under the Constitution. Although it is nowhere expressly written in, the Bill of Rights protects the privacy of exchanging ideas/beliefs in the first amendment which reads, "Congress shall make no law...prohibiting the free exercise thereof, or abridging the freedom of speech, or of the press; or the right of the people to peaceably to assemble…"[7] The Framers were apprehensive about the government having too much power while limiting the power of the people and accordingly ensured to mention in the bill of rights that cannot be taken away from citizens.

The government also tends to take a more active stance on limiting internet user privacy when it comes to criminal investigations. Because the internet stores information such as online chats and websites one visits, and can trace one's location, this information has helped prosecutors indict criminals who used the internet to commit their crime. Previously, when the government subpoenaed records from a phone company all they received were call and message logs. If the government chooses to subpoena a social media website such as Facebook, however, they get the user's profile, wall posts, photos, tagged photos of the user, their login times and IP

[7] U.S. CONST. amend. I, § 1.

data.[8] Furthermore, there is usually a GPS attached to most of the photos which can help law enforcement even more. "Ninety-one percent of today's online adults use social media regularly, which has become the number one activity on the web…"[9] meaning social media is the next best route for law enforcement to explore when it comes to investigating crimes. While this may seem as a disincentive for individuals to share certain information online about themselves, studies tend to show that people do not believe how publicly available their information truly is. "Users are often unaware of the extent to which their information is available, and if sensitive info is released, it is often impossible to put the cat back in the bag." [10]

Facebook's new facial recognition program is meant to save time when individuals upload a large amount of photos to their profile and do not want to individually tag every person.[11] The program instead suggests the person's name who is in the photo and the user only has to accept for the computer to tag the person. What started out as a time saving idea, ignited a nationwide warning on identity theft. A Carnegie Mellon professor, Alessandro Acquisti, initially became famous after reverse engineering social security numbers.[12] Now, he has developed a method that allows individuals to be identified by photo. Whether this is through a webcam or Facebook, the software uses the Facebook profile's information which is enough data

---

[8] Justin P. Murphy and Adrian Fontecilla, *Social Media Evidence in Government Investigations and Criminal Proceedings: A Frontier of New Legal Issues*, JOURNAL OF LAW AND TECHNOLOGY, http://jolt.richmond.edu/index.php/social-media-evidence-in-government-investigations-and-criminal-proceedings-a-frontier-of-new-legal-issues/ (last visited May 15, 2014).

[9] *Id.*

[10] Geoffrey A. Fowler, *When the Most Personal Secrets Get Outed on Facebook*, THE WALL STREET JOURNAL (October 13, 2012), http://online.wsj.com/news/articles/SB10000872396390444165804578008740578200224?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB10000872396390444165804578008740578200224.html.

[11] Paul Ducklin, *Facebook is Turning Facial Recognition Back On- So Here's How to Check Your "Photo Tagging" Settings*, NAKED SECURITY (Feb. 2, 2013), http://nakedsecurity.sophos.com/2013/02/02/facebook-turns-facial-recognition-back-on/.

[12] William Deutsch, *Facial Recognition(and Identity Theft) Made Easy*, BIZSECURITY.COM, http://bizsecurity.about.com/od/privacyissues/a/Facial-Recognition-And-Identity-Theft-Made-Easy.htm (last visited May 15, 2014).

to lead to identity theft. Acquisti warns that something as simple as snapping a picture and uploading it online could one day be enough to warrant a stolen identity. Social media users are now looking for a way to be able to share personal details about themselves without having the fear of strangers finding out too much about them. The problem lies with where that middle ground is. The other question is whether someone's privacy is being invaded if they voluntarily put up private information about themselves for the world to see. Users feel that they should have an expected level of privacy when they decide to enter the internet and post their opinions online, however, as it currently stands, users should post things online at their own risk with no assumption that their information is private. Anyone can access the information with as little effort as googling one's name.

Some companies are jumping on board with the large amount of users on the internet by trying to increase profits by using this information voluntarily provided by individuals online. Companies previously had to all but beg customers for feedback through surveys, phone calls, or hiring workers to ask customers face to face about their products. Now, potential customers have made it straightforward for companies to target them with specific ads tailored to their needs and wants. Rather than paying for a mass selling campaign when a company is looking for a certain type of customer, the information updated online allows companies to send out a specific ad to someone who will actually be interested in the product or service. Nestle Purina is the leading example in this type of advertising. Nestle Purina has usually been one of the first to establish a presence online with websites such as LinkedIn, Twitter and Facebook, but their new Pet Care line was looking to advertise solely to customers who had pets. [13]They established a personal connection with pet lovers first and then gradually started to promote their brand and products so

[13] Lisa Brown, *Purina Leads Pack With Personalized Social Media,* ST. LOUIS POST DISPATCH (Dec. 15, 2013), http://www.stltoday.com/business/local/purina-leads-pack-with-personalized-social-media/article_1da448e3-72d5-5052-bd13-cf3fca42b42d.html.

as not to invade in people's personal space. The campaign is a huge success and individuals respond to how much their brand loyalty has grown towards Nestle Purina. Other consumers, nevertheless, are not as thrilled with the concept of targeted advertising.

Thousands of companies are working with data brokers who "…are collecting, analyzing and packaging some of our most sensitive personal information and selling it as a commodity to each other, to advertisers, even the government, often without our direct knowledge." [14]While initially marketers vied for personal information to get a better understanding of customer needs, the volume and nature of the data has completely changed. Data mining is a multibillion dollar industry that develops files on customers storing their names, previous addresses, credit card purchases and more.[15] It is not uncommon for companies to go so far as to save one's likes and dislikes, our closest friends, our bad habits and even our daily movements. The concept of downloading information about people offline has spun out of control to the point where companies know where someone is and what they are doing even when the person is offline. Acxiom is one of the largest data brokers marketing an average of 1,500 pieces of information on over 200 million Americans.[16] What seems more suspicious is that although the company knows so much about consumers, the company itself is very secretive and refuses to answer any questions or take interviews with the media. When the public found out just how much their personal lifestyles were exposed to the corporate world, it was clear that there was no privacy available to anyone.

Tim Sarapani worked as a privacy lawyer for the American Civil Liberties Union then joined Facebook as their director of Public Policy. He speaks about the issue of privacy in

---

[14] Steve Kroft, *The Data Brokers: Selling Your Personal Information,* CBSNEWS.COM (March 2009), http://www.cbsnews.com/news/the-data-brokers-selling-your-personal-information/.
[15] *Id.*
[16] *Id.*

regards to data mining and comments that "It's not about what we know we're sharing, it's about what we don't know is being collected and sold about us."[17] Some companies even have databases about health conditions people have anything from alcoholism to depression, by tracking and plotting certain data points about individuals, the companies can now determine this information and sell it to marketers and other companies. With no regulation of these data brokers and not enough information to make them stop, people's privacy is invaded every day and they have no way to prevent it.

With so many things to consider when logging onto any account online, I would presume that internet users would be more aware and cautious when relaying their personal information to the entire world. According to a Pew Internet study, 59% of internet users do not believe it is possible to be completely anonymous online.[18] About 86% of internet users have taken some steps to minimize their digital footprints whether this be through clearing their cookies or using different names when using virtual networks.[19] Despite these efforts to take back what little is left of privacy, a survey asking internet users about problems they have experienced with stolen information, hijacked email accounts loss of reputation etc., the highest percentage at 21% goes to internet users who admit to having their email or social networking accounts taken over by someone else without their permission.[20] Out of those surveyed, most agree that more laws should be passed to protect those using the computer. Because of the fast pace technology is changing and evolving, it is nearly impossible to stay on top of everything posted online. Even

---

[17] *Id.*
[18] Lee Rainie, Sara Kiesler, Ruogu Kang and Mary Madden, *Anonymity, Privacy, and Security Online*, PEWINTERNET.ORG (Sept. 5, 2013), http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/.
[19] *Id.*
[20] *Id.*

those who have now realized that what they have online should not be seen by the public, they may delete it, but it will always remain somewhere online where others may exploit the data.

With very few federal laws relating directly to the consumers attempting to protect their privacy and sporadic state laws, a new bill has been proposed in California that may put some internet users at ease. California's Right to Know Act is not asking companies to stop collecting data on individuals since it is nearly impossible now to stop a multi-billion dollar business between companies, but they are asking to take back some privacy rights and give them back to the consumers.[21] The act would require that Google and Facebook must reveal what personal information they have collected about individuals as well as how it is being used. Opinion polls nationwide show a strong support for laws to protect our privacy online but even with strong popular support, the law has not been able to keep up and protect users because the industry has been blocking them through lobbying and large monetary donations. Civil liberties organizations, supporters and internet users have grouped together urging the legislature to take the bill seriously and pass it as soon as possible.

The strong support and urgency of individuals who want to protect our right to privacy show a generally shifting mentality in internet users. It is becoming clearer to the public that the internet is not a private place even if you intend it to be. Just because you make an album private on Facebook does not mean those pictures are solely for you and your friends to view. Minutes later, data miners already have enough information about you to sell to companies who will send you ads with items and services pertaining to your lifestyle. "After years of complacency, there are finally signs that the public is starting to demand greater privacy rights. Last week, in a long-

---

[21] Rainey Reitman, *New California "Right to Know" Act Would Let Consumers Find Out Who Has Their Personal Data-- And Get a Copy of it*, ELECTRONIC FRONTIER FOUNDATION (Apr. 2, 2013), https://www.eff.org/deeplinks/2013/04/new-california-right-know-act-would-let-consumers-find-out-who-has-their-personal.

awaited move, a powerful Senate committee endorsed an amendment to a key federal law that would give greater privacy protection by requiring the government to get a search warrant when it wants to read people's emails." [22]Even if this bill does pass, it still does not give users the opportunity to delete or correct any of their personal data. They are still powerless when it comes to stopping the sale of their data to other companies.

It seems the only way to ensure that one's data is not being compromised is to never access the internet, which is not a realistic solution as our society is traveling deeper towards a complete digital state used by billions. It is apparent that there is an invasion of our privacy happening and it goes beyond the voluntary information we put online and stems towards the information that is inferred about us and the patterns companies piece together by tracking our every move and purchase. I will not argue that the government should have no say in tracking the internet when it comes to my personal safety or the safety of the entire nation. As I see it, the same applies to criminal investigations where the internet has sensitive data that can be used to bring justice and peace to someone who was wronged. Nevertheless, I consider that there is a decreasing standard of privacy and what that means for internet users. Internet users are now aware of their publicity online and recognize they need to be cautious, but the problem ensues when they do not know what information truly is safe to put online. With so little as an uploaded picture creating the possibility of a security breach it seems unavoidable for the government to become more involved in preserving citizen's individual rights to their personal content as it is impossible to completely avoid technology all together. As a rule, it is probably safest not to post anything online that you would not share with a stranger and keep as low of a profile as possible to protect your privacy as best as you can.

---

[22] Adam Cohen, *Internet Privacy: A New Bill Finally Offers Protections,* TIME (Apr. 30, 2013), http://ideas.time.com/2013/04/30/internet-privacy-a-new-bill-finally-offers-protections/.

Finding Friends: Data Privacy in the United States and the European Union

Ashley Johann

Friend Finder

Facebook offers a vast database of people, both known and unknown, to every new user. After registering for a Facebook account, how can a user possibly comb through the millions of existing profiles in order to locate the people they know personally? Facebook has an answer to this question: the Friend Finder feature. Friend Finder allows a user to upload contact data from another service, such as email, through which Facebook can mine for potential friends.[23] Facebook users can then look at the list created from this process and select any current users to add as friends or non-users to invite to join Facebook.[24]

Some may find this feature attractive, but the Federation of German Consumer Organizations ("VZBV") recently challenged Facebook's Friend Finder tool in German court. In its February 2014 decision, the Higher Court of Berlin ruled that certain aspects of the tool violate German law.[25] In a previous version of the tool, acceptance of Facebook's privacy policy included permission for Facebook to access the users' contact information, send emails to friends who were not currently using Facebook, and share the data with unspecified third parties.[26] VZBV argued that users were not properly informed of these permissions, and the court agreed. The court also ruled that Facebook's use of non-users' personal data for the purposes of personalized advertising was illegal, as the targeted individuals had not given consent to receive

---

[23] *Finding Friends*, FACEBOOK, https://www.facebook.com/help/findingfriends (last visited Apr. 4, 2014).
[24] *Id.*
[25] Loek Essers, *Facebook Must Comply with German Data Protection Law, Court Rules*, PC WORLD (Feb. 18, 2014, 4:05 AM), http://www.pcworld.com/article/2098720/facebook-must-comply-with-german-data-protection-law-court-rules.html.
[26] *Facebook Subject to German Data Protection Rules, Says Berlin Court*, OUT-LAW.COM (Feb. 26, 2014), http://www.out-law.com/en/articles/2014/february/facebook-subject-to-german-data-protection-rules-says-berlin-court/.

the advertising.[27] With Facebook being a U.S.-based company, this case in Germany brings to light the stark differences between data privacy laws in the United States and Europe. This paper seeks to contextualize this case through a brief examination of United States and European (specifically German) privacy law, as well as some points of contrast and potential reconciliation between the two jurisdictions.

Privacy in the United States

Although some other United States government organizations have taken actions, the Federal Trade Commission ("FTC") remains the main player, so to speak, in regards to privacy law in the U.S. The FTC has used its powers to enforce the privacy policies of social media networks, to suggest a universal "do not track" feature online that would alert consumers to what data was being tracked and when,[28] and to impose 20-year consent orders for FTC monitoring on sites such as Facebook, Twitter, MySpace, and Google.[29]

Facebook's consent order from the Federal Trade Commission contains ten parts, which delineate actions that the FTC deemed necessary for Facebook to take in response to an official FTC complaint against their privacy and advertising policy.[30] The Complaint alleged that Facebook did not clearly explain privacy policies to users and that Facebook gave third parties access to user information without the users' knowledge or consent.[31] Accordingly, the consent order contains a demand that Facebook may not expressly nor by implication misrepresent privacy or security of information.[32] The order also declared that when sharing information with third parties, Facebook must "clearly and prominently disclose" to the user: "(1) categories of

---

[27] *Id.*
[28] Laura Ybarra, *The E.U. Model as an Adoptable Approach for U.S. Privacy Laws: A Comparative Analysis of Data Collection Laws in the United Kingdom, Germany, and the United States*, 34 LOY. L.A. 267, 278 (2011).
[29] Theodore F. Claypool, *Privacy and Social Media*, AMERICAN BAR ASSOCIATION: BUSINESS LAW TODAY, http://www.americanbar.org/publications/blt/2014/01/03a_claypoole.html (last visited Apr. 4, 2014).
[30] Facebook, Inc., 2012 FTC LEXIS 135 (F.T.C. July 27, 2012).
[31] Facebook, Inc., 2012 FTC LEXIS 136 (F.T.C. July 27, 2012).
[32] FTC Consent Order, *supra* note 30.

nonpublic user information that will be disclosed…(2) the identity or specific categories of such third parties, and (3) that such sharing exceeds the restrictions imposed by the privacy settings in effect for the user."[33]

Even though the FTC is taking a role in data privacy regulation, their orders extend only to specific companies in specific situations. Overall, the United States approach to data privacy is extremely fragmented. For example, in just the realm of electronic data alone, regulation may fall under The Children's Online Privacy Protection Rule, the Children's Internet Protection Act of 2001, the Federal Information Security Act, the Electronic Communications Privacy Act of 1986, the Electronic Freedom of Information Act, or the USA PATRIOT Act of 2001, to name just a few.[34]

In light of the lack of federal statutory regulation, many states have enacted privacy laws of their own. For example, twelve states restrict employers' access to their employees' social media accounts, and a California law requires sites to disclose whether or not they honor "do not track" instructions from internet browsers.[35]

The State of California has taken a particular interest in privacy regulation, and has established the Department of Justice Privacy Enforcement and Protection Unit to Advise the California Attorney General on issues related to privacy.[36] This unit also "enforces state and federal privacy laws," provides resources for consumers, and works with businesses to make recommendations and offer guidelines.[37]

---

[33] *Id.*
[34] *See United States Privacy Laws*, INFORMATIONSHIELD, http://www.informationshield.com/usprivacylaws.html (last visited Apr. 4, 2014).
[35] Claypool, *surpa* note 29.
[36] *See Privacy Enforcement and Protection*, STATE OF CALIFORNIA DEPARTMENT OF JUSTICE: OFFICE OF THE ATTORNEY GENERAL, http://oag.ca.gov/privacy (last visited Apr. 4, 2014).
[37] *Id.*

In addition to the FTC and individual states' regulations, privacy law in the United States also derives from case law, particularly class-action lawsuits. One such case from the United States Court of Appeals for the Ninth Circuit, *Lane v. Facebook, Inc.*, provides persuasive authority against advertising programs such as Facebook's Beacon program, which was discontinued in the *Lane* settlement.[38] Beacon disclosed user purchases and other private information without user consent. In the settlement, Beacon was discontinued, and a portion of Facebook's payouts went toward the establishment of the Digital Trust Foundation to advance the areas of internet privacy and security.[39]

In order to help alleviate some of the fragmentation in data privacy law, in 2012, the White House called for a sort of "Privacy Bill of Rights" to provide a broad base of government protection. This proposal has seven features that are designed to provide overarching regulation in the area of data privacy: (1) "Individual control" over what data is collected and how it is used, (2) "Transparency," or the right to comprehensible information about a company's privacy practices, (3) "Respect for [the] context" in which the data is collected, meaning that data should be used in a manner consistent with that context, (4) "Security" of the data collected, including control of risks such as loss and unauthorized access, (5) "Access and accuracy," defined as the consumer's right to correct data or request its deletion, (6) "Focused collection" of personal data only when it is absolutely necessary, and (7) "Accountability" to enforcement agencies to ensure that all consumers retain all the protections guaranteed by the Privacy Bill of Rights.[40] If the Privacy Bill of Rights were to be enacted, it would provide straightforward, comprehensive data protection similar to that seen in Europe.

---

[38] Lane v. Facebook, Inc., 696 F.3d 811, 811 (9th Cir. 2012).
[39] Lane v. Facebook, Inc., 696 F.3d 811, 817 (9th Cir. 2012).
[40] *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, THE WHITE HOUSE 47-48 (Feb. 2012), http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

Despite calls for comprehensive regulation, no such laws have been put into practice. The reason may be confusion. Thomas H. Davenport of the *Wall Street Journal* argues that the issue is too complex for Congress to handle, and argues that free flow of information is necessary for corporate innovation.[41] It may also be cultural. Davenport notes, citing extensive use of social media as evidence, that online privacy is not a priority for most Americans.[42]

Privacy in the European Union

In contrast to the United States' patchwork approach to privacy law, privacy in Europe is specifically defined and regulated. In a Wall Street Journal article, Joel R. Reidenberg states, "Europe's system recognizes that privacy, regardless of context, is a core democratic value that must be safeguarded, not left to market forces."[43]

The European Convention on Human Rights provides the overarching framework for European privacy law, as it addresses the "Right to respect for private and family life" as a right and freedom that all signatories must protect.[44] It demands, "Everyone has the right to respect for his private and family life, his home and his correspondence," and goes on to say no public authority should interfere with this right except in accordance with the law when it is absolutely necessary.[45] Laws promulgated in European countries that are signatories to the European Convention on Human Rights originate from the perspective of privacy as a basic human right.

For European Union member states, privacy laws are based on European Union Directives, which allow for individual countries to create their own laws, as long as they keep

---

[41] Thomas H. Davenport & Joel R. Reidenberg, *Should the U.S. Adopt European-Style Data-Privacy Protections?*, THE WALL STREET JOURNAL (Mar. 10, 2013, 4:00 PM), http://online.wsj.com/news/articles/SB10001424127887324338604578328393797127094.
[42] *Id.*
[43] *Id.*
[44] European Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, 213 U.N.T.S. 221, *available at* http://www.echr.coe.int/Documents/Convention_ENG.pdf.
[45] *Id.*

with the principles of and achieve the result of the directive.[46] Under the EU Directive, personal data is defined as: "any information relating to an identified or identifiable natural person…who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physiological, mental, economic, cultural, or social identity."[47] According to Paul M. Schwartz, The EU directive has three main goals: "(1) to facilitate the free flow of personal data within the EU, (2) to ensure an equally high level of protection within all countries in the EU for the fundamental rights and freedoms of natural persons, and in particular their right to privacy; and (3) to protect the privacy of the information of EU citizens worldwide by blocking data transfers to 'third countries' that lack 'adequate protection.'"[48] The directive requires that all member states "create a supervisory authority to monitor the state's compliance with the directive."[49] Although the EU directive is straightforward and unifying, it still allows for wide differences in privacy policy and enforcement across Europe. Germany is known for being the most strict regarding privacy laws, while the United Kingdom is known as the most liberal.[50]

In the interest of examining specific European laws that apply to the Facebook case under discussion, it is necessary to examine the German Federal Data Protection Act, as well as a few more specific provisions in the European Union's directive. Section 4(1) of Germany's Act states that the collection of data is only lawful "if permitted or ordered by this Act or other law."[51] Section 4(3) goes on to describe the specific conditions for data collection:

> If personal data are collected from the data subject, the controller shall inform him/her as to
> 1. the identity of the controller,

[46] Ybarra, *supra* note 28 at 280-281.
[47] Council Directive 95/46/EC, art. 2, 1995 O.J. (L 281).
[48] Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966, 1972 (2013).
[49] Ybarra, *supra* note 28 at 281.
[50] *See id.*at 285.
[51] Bundesdatenschutzgesetz [German Federal Data Protection Act], Jan. 14, 2003, BGBL I at 2814, § 4(1).

2. the purposes of collection, processing or use, and
3. the categories of recipients only where, given the circumstances of the individual case, the data subject need not expect that his/her data will be transferred to such recipients,

unless the data subject is already aware of this information.[52]

The European Union directive 1995/46/EC, Article 4(1)(c) stipulates that member states should apply their own legal provisions when the data controller is located outside the member state, but uses hardware within the state to process data.[53]

Contrasting Jurisdictions

Taking into account the FTC's monitoring consent order with Facebook and class action lawsuits such as *Lane*, it is evident that U.S. law is moving toward similar requirements as the European Union. Both jurisdictions emphasize notice of and consent to the collection of personal data. European jurisdictions such as Germany have a more straightforward approach, delineating requirements in general bodies of law such as EU Directives and Germany's Federal Data Protection Act.

Although the end goals and results are similar, these two jurisdictions do have differences. Unlike the European Union, the United States does not place legal limits on the exportation of data abroad.[54] Also, while the U.S. only puts limited importance on "notice of data processing practices," the European Union has a much more inclusive focus: data collection limits, "the data quality principle," and "notice, access, and correction rights for the individual."[55] Europe also forbids the collection of data that is not specifically provided for in the law.[56] The U.S. on the other hand, only forbids the collection of data that is specifically named in

---

[52] *Id.* at § 4(3).
[53] Council Directive 95/46/EC, art. 4, 1995 O.J. (L 281).
[54] Schwartz, *supra* note 48 at 1977.
[55] *Id.* at 1976.
[56] *Id.*

the law.[57] In other words, while the European Union makes laws about what *can* be collected, the U.S. makes laws about what *cannot*. Differences such as these account for instances like the recent Facebook case, where German law prohibits a feature such as Facebook's Friend Finder that encounters little legal opposition in the United States.

Because it is a U.S.-based company, Facebook bases its privacy policy in U.S. law, which, compared to Germany's law allows for greater corporate freedom as to the use of personal data. Although Friend Finder is technically legal in the United States, German law is applicable in the case under discussion because of the European Directive provision that requires all third countries to have "adequate" data protection.[58] Since the laws in Europe and the United States are so different, a company like Facebook is certain to run into problems if they apply U.S.-based policies to business operations in Germany. German law, as seen in § 4(3) of the German Federal Data Protection Act, is very specific in delineating the conditions under which data may be collected and how the consumer must be informed.[59] The case against Facebook alleged that it was these notification rules, which are more strongly present in German law than U.S. law, that were violated.[60] Unless they file an objection against the ruling, Facebook must now, at least for German customers, adjust the Friend Finder feature and related privacy notices to comply with German law.

Similar cases in which a U.S. company's data protections did not hold up against European law have led to various joint efforts toward achieving "adequacy,"[61] as well as efforts to adjust laws and policies so that they become acceptable for international business.

Potential Responses

---

[57] *Id.*
[58] *Id.* at 1973.
[59] Bundesdatenschutzgesetz [German Federal Data Protection Act], Jan. 14, 2003, BGBL I at 2814, § 4(3).
[60] *Facebook Subject to German Data Protection Rules, Says Berlin Court, supra* note 26.
[61] Schwartz, *supra* note 48 at 1967.

The privacy collision between Facebook and Germany discussed here is illustrative of most of Europe because all European Member States' laws are based in the same set of Directives. Given the differences between United States and European laws it is evident that some response, either by government or businesses, is necessary in order to close this divide and allow for greater ease of international business. On a governmental level, the United States could respond by changing its privacy laws to more closely match that of other countries. This is a rather large undertaking though, and given the current state of privacy legislation, there is a place for concerns like those of Davenport that the issue may be too complex. Perhaps government resources and energy are best spent in other areas.

The most effective response may come from businesses themselves. Companies understandably tend to follow the least stringent applicable laws, but some are proposing that this may not be a wise course of action anymore.[62] Schwartz asserts that European policies could become adopted "de facto." Although the United States Congress has not officially adopted the policies, companies might choose to comply with them in order to maintain "adequate" protections internationally.[63] If companies adopt the most stringent applicable privacy laws as their policies, they will not only be aiding themselves legally in foreign jurisdictions, but also contribute to reform in U.S. privacy law through market forces. However, to be completely realistic, adopting stricter overarching privacy policies without real legal incentive from a business's country of incorporation seems to characterize a kind of privacy "overachievement" that is unlikely to occur. For the time being, if they wish to avoid legal action, companies like Facebook will have to adjust their privacy policies to comply individually with each country in which they do business.

---

[62] *See Facebook Must Comply with German Data Protection Law, Court Rules, supra* note 25.
[63] See Schwartz, *supra* note 48 at 1987.

THE "GENE"RAL PRIVACY PROBLEM: AN ARGUMENT AGAINST THE MARYLAND V. KING DECISION

Caitlan Grombka-Murphy

Through developments in science and technology, researchers continue to reveal new insights and milestones in genetics. Among the highlights are the first discovery of DNA in 1869, Watson and Crick's double helix model in 1953, and the sequencing of the human genome in 2003.[64] Not only have discoveries concerning DNA been valuable to the field of science, but they also have made significant contributions to the law enforcement system, especially in criminal profiling. With DNA collection and profiles, law enforcement officials are able to solve crimes with exponentially greater accuracy.[65] For example, law enforcement might collect and analyze DNA from: (1) blood, saliva, semen, and tissue found at crime scenes; (2) the remains of unidentified persons or relatives of missing persons; (3) people convicted of various crimes; and (4) persons arrested for various crimes.[66] The Maryland DNA Collection Act, which has recently generated enough controversy to warrant judicial scrutiny, pertains to the fourth way law enforcement might use DNA. The 2008 amendment to the Maryland DNA Collection Act authorized the collection of DNA by a buccal (cheek) swab from people arrested for burglary or violent crimes upon their arrest, prior to being found guilty or pleading guilty.[67] The DNA database profile of an arrestee greatly benefits law enforcement's core goal of crime solving by

---

[64] *Genetic Timeline,* NATIONAL HUMAN GENOME RESEARCH INSTITUTE (Sept., 27, 2011), http://www.genome.gov/pages/education/genetictimeline.pdf.
[65] *Using DNA to Solve Crimes,* U.S. DEPARTMENT OF JUSTICE (March 2003), http://www.justice.gov/ag/dnapolicybook_solve_crimes.htm.
[66] *Combined DNA Index System (CODIS),* F.B.I., http://www.fbi.gov/about-us/lab/biometric-analysis/codis/codis-and-ndis-fact-sheet.
[67] *King v. State*, 42 A.3d 549, 552 (2012).

perhaps generating a positive match of the arrestee to past-unsolved crimes or to future crimes, regardless of whether he or she is guilty or not guilty of the presently charged offense.[68]

Such advancements in the understanding of DNA, however, do not arise without cost. One prominent issue regarding DNA in criminal profiling, especially the use of arrestee DNA, is attempting to strike a balance between a useful modernized crime investigation technology and the individual's fundamental Fourth Amendment rights. The Fourth Amendment says that people have a right "to be secure in their persons, homes, papers, and effects against unreasonable searches and seizures."[69] Courts have found DNA collection to constitute a "search" under the Fourth Amendment.[70] Since individuals are protected against unreasonable search and seizure under the Fourth Amendment, the question on balance, then, is whether a DNA collection "search" of an arrestee is "unreasonable" and therefore unconstitutional.

Maryland v King, a Supreme Court Case, tackled the balance issue, ruling that DNA profiling by buccal swab is such a useful crime-fighting technology that the threat to an individual's right to privacy is not constitutionally unreasonable**.**[71] In a 5-4 decision, the Supreme Court of the United States held that the warrant-less collection of DNA via a buccal swab from Alonzo King upon his arrest was a legitimate search procedure, reasonable under the Fourth Amendment because it was only a "minimal" violation of his privacy.[72] In this essay, I will explain the background of *Maryland v King,* refute the Court's reasoning, and then go on to argue that the court erred in their decision for main three reasons. I will show that the court failed

---

[68] Josh Gerstein & Darren Samuelsohn, *SCOTUS Upholds DNA Testing for Serious Arrests,* POLITICO (June 3, 2013).
[69] Brief of Petitioner at 2, Maryland v. King 133 S. Ct. 1958 (2013) (No. 12-207).
[70] Maryland v. King, 133 S. Ct. 1958, 1966 (2013).
[71] Elizabeth E. Joh, *Maryland v King: Three Concerns about Policing and Genetic Information,* GENOMICS LAW REPORT (Sept. 19, 2013), http://www.genomicslawreport.com/index.php/2013/09/19/maryland-v-king-three-concerns-about-policing-and-genetic-information/.
[72] *Maryland*, 133 S. Ct. at 1958.

to: (1) adequately acknowledge that King's DNA was not used for identification purposes, (2) show concern that DNA samples contain more than a person's identity, and (3) recognize the decision's future implications, ultimately arguing that DNA collection under the Maryland DNA Collection Act is an unreasonable search under the Fourth Amendment.

On April 10, 2009, police arrested Alonzo King and charged him with assault for threatening a group of people at gunpoint.[73] Officials subsequently obtained a DNA sample from him in the form of a cheek swab and, and about three months later entered it into the CODIS DNA database.[74] The DNA analysis showed a positive match between King's sample and a sample gathered from an unsolved sexual assault from 2003.[75] The match provided the police with probable cause to indict King on ten charges, including rape.[76] The police also acquired a search warrant to conduct a second buccal swab DNA sample to be obtained for verification.[77] Upon the second positive match, King was convicted of rape and sentenced for life without parole.[78]

Unsuccessful at trial and appellate court, King appealed his decision to the Maryland Supreme Court. King argued that the DNA collection was a violation of his Fourth Amendment rights and that the Maryland DNA Collection Act was unconstitutional.[79] Using the "totality of the circumstances" test, the Maryland Supreme Court weighed the intrusion upon King's privacy against the government's interest in apprehending criminals, concluding the Maryland DNA Collection Act to be unconstitutional.[80] The court reasoned that an arrested person still has the

---

[73] 42 A.3d at 552.
[74] *Id.*
[75] *Id.*
[76] *Id.*
[77] *Id.*
[78] *Maryland v. King,* ELECTRONIC PRIVACY INFORMATION CENTER, https://epic.org/amicus/dna-act/maryland/ (last visited May 15, 2014).
[79] 133 S. Ct. at 1958.
[80] *Id.*

presumption of innocence and therefore retains strong privacy rights.[81] Furthermore, the court reasoned that although "solving cold cases is a legitimate government interest, a warrantless, suspicion-less search cannot be upheld by a 'generalized interest' in solving crimes."[82] The State of Maryland appealed the decision to the Supreme Court. The Supreme Court then considered the question of whether the privacy intrusions allowed by the Maryland DNA Collection Act were "unreasonable searches" prohibited by the Fourth Amendment.

In order to decide whether the privacy intrusion under the Maryland DNA Collection Act is reasonable or unreasonable, one must look at how DNA collection works under the Act. Once a DNA sample is obtained from the arrestee via a buccal swab, thirteen short-tandem-repeats of "non-coding" DNA are used in a polymerase chain reaction (PCR), which amplifies the DNA for analysis.[83] After analysis and the first scheduled arraignment date, the DNA profile is uploaded to the state DNA or FBI CODIS databases and stored.[84] If a match is attained between the newly-entered sample and a previously stored profile, the police can use this match as evidence in their application for a warrant for a second DNA sample to be taken and used as evidence in court.[85]

The U.S. Supreme Court ruled in favor of the constitutionality of the Maryland DNA Collection Act in light of the Fourth Amendment, reversing the decision of the Maryland Supreme Court.[86] The U.S. Supreme Court reasoned that an intrusion on an arrestee's right to privacy in DNA collection is justified and reasonable because (1) such DNA collection improves the criminal justice system, (2) only identity information is given, (3) criminal history is a critical part of a person's identity, and (4) a buccal swab requires no intrusion beneath the skin.[87] The

---

[81] 42 A.3d at 552.
[82] *Id.*
[83] *Id.*
[84] *Id.*
[85] *Id.*
[86] 133 S. Ct. at 1958.
[87] *Id.*

Court determined that because an arrestee is already in custody, and the police were required to have probable cause to make the arrest, the search amounts to "reasonableness."[88] In balancing the "reasonableness" of the DNA collection practice, the court determined that greater weight is given to the government interest in the identification of an arrestee than the privacy rights of the individual, and that DNA has the potential to serve this interest.[89]

The Supreme Court expanded on its first line of reasoning saying that an intrusion on an arrestee's right to privacy in DNA collection is reasonable because it improves the criminal justice system *by* identifying the suspect with certainty.[90] It is important to note here that the court does not hold that DNA collection improves the criminal justice system by solving crimes, but rather by identifying a suspect with certainty. We must then ask the question: is DNA analysis the best way to identify a suspect with certainty? DNA analysis can work to both solve crimes and identify persons, however, the sole purpose fingerprint analysis is identification.[91] Moreover, fingerprint analysis takes about 27 minutes to confirm a person's identity, whereas DNA analysis takes months.[92] The difference in processing time shows that even if DNA was used to match up names and biological traits, it would not be the most efficient method.

The second reasoning that the Supreme Court used is that an intrusion on an arrestee's privacy in DNA collection is reasonable because it is used only for identifying information. This brings us to the question: what does the DNA analyzed actually contain? DNA samples contain much more personal information than fingerprints. Although noncoding DNA is often called "junk DNA" because it does not encode for a person's genes directly, it does serve a function in

---

[88] *Id.*
[89] *Id.*
[90] *Id.*
[91] Robert Barnes, *Supreme Court weighs DNA 'Fingerprinting',* WASHINGTON POST (Feb. 26, 2013) http://www.washingtonpost.com/politics/supreme-court-weighs-dna-fingerprinting/2013/02/26/5eb3c5b6-804e-11e2-b99e-6baf4ebe42df_story.html.
[92] 133 S. Ct. at 1958.

DNA replication and cell division.[93] Genetic science shows a trend toward finding ways to use "junk DNA," and in the future, non-coding DNA will likely reveal more personal information about us, including our susceptibilities to disease and behaviors.[94]

The Court's discussion primarily rests on "identity." Generally, "identifying" someone means finding out who they are based on physical properties. For example, height, weight, skin color, hair color, and eye color all identify a person. If a person steals another's identity, he or she takes the other's height, weight, skin color, hair color, and eye color and items that go along with this like a license, credit card, and social security number. The court seems to use "identify," however, in a different and unfamiliar way. The Court's definition of identification, on the other hand, links the individual to past behavior; they state that criminal history is a crucial part of a person's identity.[95] The worry then is whether criminal history found by DNA be part of a person's identity. With identity theft, it is not.

The Court's point is that DNA collection is a minimally invasive procedure akin to fingerprinting and is therefore reasonable. Although DNA sampling is not painful or harmful because it does not involve intrusion beneath the skin, it is significantly more invasive than a simple fingerprint. In DNA sampling of arrestees under the Maryland DNA Act, a cotton swab must enter the mouth and scrape the inner cheek of the arrestee.[96]

In *Maryland v. King,* the Supreme Court erred in their decision for three main reasons. First the Court failed to acknowledge that King's DNA was not used for identifying purposes. Second, the Court failed to show concern that DNA samples contain more than a person's

---

[93] Brief of Amici Curiae Electronic Privacy Information Center and Twenty-six Technical Experts and Legal Scholars in Support of Respondent at 14, Maryland v. King, 133 S. Ct. 1958 (2013) (No. 12-207).
[94] *Id* at 15.
[95] 133 S. Ct. at 1958.
[96] *Id.*

identity. And third, the Court failed to recognize the decision's future implications on the criminal justice system.

First, King's DNA was never actually used to identify him, but rather to discover an unknown crime he had committed. The Maryland DNA Collection Act states that the DNA cannot be submitted to the database until an arraignment is scheduled.[97] That being said, it was about four months after the sample had been taken that King's DNA showed a link to the 2003 rape.[98] By this time, King had already been given a set bail, engaged in discovery, and requested a speedy trial.[99] Since the Fourth Amendment prohibits searching when there is no basis for believing a person is guilty, the court justifies this DNA "search" by saying it contributes to the proper identification process.[100] However, the court improperly broadens the attributes that "identification" can encompass. The way that DNA analysis works, thus, is by "identifying" or matching persons based to past-unsolved crime. DNA database matching "identifies" an individual in the way the way that the police would "identify" the perpetrator of a crime by searching every house in a neighborhood. This kind of "identification" is indistinguishable from suspicionless searches, which we know are unconstitutional.[101] Since there was no actual suspicion that King committed the 2003 rape or any other unsolved crimes in the database, it follows that the privacy intrusion is not justified. Furthermore, the DNA search, in King's case, does not seem to have "contributed to the proper identification process" because it was performed four months later to link him to an unsolved crime, not to identify him.

Second, the Court failed to show concern that DNA samples contain more than a person's identity. As I have touched upon, developments in technology will allow more and more

---

[97] MD. CODE ANN., PUB. SAFETY § 2-504 (West 2014).
[98] 133 S. Ct. at 1958.
[99] *Id.*
[100] *Id.*
[101] *Id.*

personal information to be extracted from non-coding DNA. Some of these uses of "junk-DNA" are emerging already. One present concern is that the 13 CODIS loci used for DNA analysis allows the identification of a person's race, ethnicity, and heritage, since different ethnic groups have distinctive patterns at these 13 loci.[102] Another present concern is that the ability to search for matches compromises the privacy of close relatives of the arrestee as "partial matches" to the sample are likely to be flagged.[103] A final worry is that there are no federal statutes that require law enforcement personnel to discard the entire DNA sample that is originally taken from an arrestee.[104] This indefinite retention of DNA samples allows for indefinite access to personal information and the potential for problems if the database is ever compromised or exploited.[105]

Finally, the Court failed to realize the grave consequences of this case both on future law enforcement practices and on logistical privacy practices. One concern is that permitting DNA collection as a common procedure allows DNA to be collected whether a person is arrested, rightfully or wrongfully, and for any reason.[106] This places a severe burden on DNA databases because of the sheer number of samples and profiles.[107] For example, a recent study showed that one third of the American population is arrested by the age of twenty-three.[108] One worry with an overburdened database is the higher possibility for compromised security. Another worry is the cost. If officials took DNA samples from the entire United States population, the test alone would cost close to $670 million dollars, not including the additional costs of extra personnel,

---

[102] Brief of Amici Curiae, supra note 93 at 13.
[103] *Id.* at 2.
[104] *Maryland v. King,* ELECTRONIC PRIVACY INFORMATION CENTER (2013), https://epic.org/amicus/dna-act/maryland/.
[105] Dan Cossins, *Supreme Court Oks DNA Collection on Arrest,* THE SCIENTIST (June 4, 2013).
[106] Josh Gerstein and Darren Samuelsohn, *SCOTUS Upholds DNA Testing for Serious Arrests,* POLITICO (June 3, 2013).
[107] Brief of Amici Curiae, supra note 93 at 2.
[108] *Viewpoints: Supreme Court and DNA Samples,* BBC NEWS (June 3, 2013).

training, equipment, and laboratory space.[109] Although it is not the primary job of the Supreme Court to make a decision based on the future benefits of a decision, but rather on the constitutionality of a law, historically speaking, courts have often looked to the implications of their decision especially if they lean towards breaking precedent.[110] In the words of Justice Breyer, "the Court should interpret written words using traditional legal tools, such as text, history, tradition, precedent, and, particularly, purposes and related consequences, to help make the law effective."[111]

In my arguments above, I have shed light on three major flaws in the court's reasoning. First, the failure of the court to recognize that DNA profiling is not for identification, second, the failure of the court to show concern for the amount of information DNA contains, and third, the failure of the court to recognize the future implications of DNA profiling on the criminal justice system. Instead of emphasizing the physical privacy aspects surrounding DNA collection, I believe the court should have used this case more as an opportunity to address informational privacy. As technology, not just with genetics, but with other fields too, advances and expands, there is going to be a continual conflict with our Fourth Amendment Right to Privacy. There will definitely be a time, most likely in the near future, when these two great things—our technology and our privacy—will again face the courts. And perhaps, in time, we can achieve some *gene*ral privacy.

---

[109] Kelly Ferrell, *Twenty-first Century Surveillance: DNA "Data-Mining" and the Erosion of the Fourth Amendment*, 51 HOUS. L. REV. 229, 245 (2013).
[110] *See* INTERPRETING PRECEDENTS: A COMPARATIVE STUDY (Niel MacCormick & Robert S. Summers eds.,1997).
[111] Nina Totenberg, *History Through a Supreme Court Justice's Lens,* NPR (Sept. 13, 2010).

The Fourth Amendment: From a Malleable Standard to a Uniform Rule

Petina Benigno

The fifty-four words of the Fourth Amendment contain a general ground for jurisprudence, but the Amendment creates more interpretable questions than truth of standard. Judges and civilians alike search for a secure affirmation of their Fourth Amendment rights. However, this amendment has attained a growing ambiguity in the past two-and-a-quarter centuries, with judges have setting roots of precedent that branch many directions and entwine with many legal theories, both convergent and divergent. The ambition of this article is to set clear definitions of the Fourth Amendment and to encourage uniformity. This will maximize economic efficiency and minimize social costs. More specifically, an antecedent modern-day Fourth Amendment rule would result on a holistic decision that maximizes the control of crime and the effectiveness of evidence and minimizes social threats to privacy. As it is now, the interpretation and adjudication of the Fourth Amendment is a malleable standard. It should rather be shifted to a living constitutional rule establishing an ex ante precedent that promotes economic and social well-being.

> *The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures, shall not be violated…*

In other words, people of the United States[112] have the right to a "reasonable expectation" of privacy.[113] The goal and original purpose is to deter violations of privacy from happening in the first place, particularly in the form of police action. Yet, there are "trends in the Fourth

---

[112] *See, e.g.,* United States v. Verdugo-Urquidez, 494 U.S. 259, 259 (1990). This case stands for the proposition that in the Fourth Amendment, the words, "the people" has a particular meaning. "Aliens who are lawfully present in the United States are among those people who are entitled to the protection of the Bill of Rights, including the Fourth Amendment." *Id*. at 279 (Stevens, J., concurring). However, that protection does not apply to the "search and seizure by United States agents of property that is owned by a nonresident alien and located in a foreign country." *Id.* at 261.

[113] *See e.g.* Katz v United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring) ("[A] person has a constitutionally protected reasonable expectation of privacy.")

Amendment doctrine that threaten to undermine this protection."[114] Legal conversation buzzes around the interpretations of words, potential dual interpretation of cases, or divergent precedent. It is figuratively as though a case enters a maze upon the first filing and has certain checkpoints, u-turns, and zig-zags that determine the right basis for judgment. Was there a search? Yes? Move one space to this checkpoint. Was it legal with a warrant? Probable cause? No, yes. Move one space under this interpretation of the amendment. Then, based on answers to these questions and checkmarks, the judge can make a decision on the case. Thus, the interpretation and adjudication of the Fourth Amendment has become that of an ex post standard, rather than an ex ante rule.

Choosing between rules and standards presents an argument on ex ante approaches and ex post approaches to thinking about the law. A *standard* requires a judgment of the facts before it is used – much like answering the questions in the checkpoint maze mentioned above. On the other hand, the consequences of a *rule* are triggered once all of the facts are settled; a rule requires precision, and it is clear in appearance but crude in its application.[115] It follows that standards align with an ex post perspective of logic, while rules trigger ex ante logic. Ex post perspectives involve looking back at an event after it has occurred and deciding then how to solve a problem, much like how standards provoke decisions based on the application of past conduct and past decisions that evoked the conduct. On the contrary, ex ante decisions are forward looking and ask what effects the decision about the case will have in the future – on parties who are entering similar situations and have not yet decided what to do, and whose choices may be influenced by the consequences the law says will follow from them. Rules are set in advanced to maximize the benefits of the situation; they set a clear guideline of which to

[114] Bryan D. Lammon, *The Practical Mandates of the Fourth Amendment: A Behavioral Argument for the Exclusionary Rule and Warrant Preference*, 85 WASH. U. L. REV. 1101, 1101 (2007).
[115] WARD FARNSWORTH, THE LEGAL ANALYST: A TOOLKIT FOR THINKING ABOUT THE LAW (2007).

abide. Giving society clear regulation and consequence makes it easier to comply with, adjudicate on, and maximize the efficiency of the law.

The "reasonableness clause", the "exclusionary rule", and the "warrant clause" are all interpretations of the Fourth Amendment.[116] The essential purpose of the Fourth Amendment is to protect peoples' rights to privacy from government interference. An important question to ask, then, is what limits does the government have regarding a person's right to privacy? In Katz v. United States, one of the earlier Fourth Amendment cases, the courts established a theory regarding a reasonable expectation of privacy.[117] The plaintiff, Mr. Katz, was indicted for transmitting wagering information by telephone in violation of 18 U.S. Code § 1084, which relates to compensation through bets and wagers through wire transmission.[118] Federal agents attached a listening device to the outside of a telephone booth often used by Katz. In the lower court the evidence of the recorded phone conversation was allowed, based on the court's finding that the federal administration did not conduct a search.[119] The decision to allow the evidence was then overturned on appeal by the Supreme Court stating that the listening device consisted of a search and seizure under the Fourth Amendment. In this case, Justice Harlan established a two part test for the right to privacy. The first part is that a person must hold an actual expectation of privacy and the second is that this expectation must be recognizably reasonable by a consenting society.[120] By extension, this landmark ruling and reasonableness test allowed reasonable people to visualize the future and see the important circumstances surrounding a particular case. The reasonable person, ideally, would know the consequences of his or her

---

[116] JOSHUA DRESSLER & GEORGE C. THOMAS, CRIMINAL PROCEDURE: PRINCIPLES, POLICIES, AND PERSPECTIVES (5th ed. 2012).
[117] *See Katz,* 389 U.S. at 360.
[118] 18 U.S.C. § 1084 (2012).
[119] The decision of the lower court was based on Supreme Court precedent in Olmstead v. United States 277 U.S. 438, 438 (1928).
[120] *See Katz*, 389 U.S. at 361.

actions. This is one example of how divergent opinions muddy the clarity of the fundamental intent of the Fourth Amendment. Different courts, different time periods, and different opinions presented two different interpretations on the law; one can see how this creates confusion and lack of clear boundary lines to follow. Ignorance aside, citizens and lawmakers alike should know what the law is before action is taken, and thus the creation of a clear rule can only make society more efficient.

And no warrants shall issue but upon probable cause, supported by oath, or affirmation.

The concept of probable cause stems from the reasonableness clause and further adds to the potential for varying opinions on judgments. Probable cause is defined as having a reasonable basis for believing the crime may have been committed or having the presence of some exigent circumstance that would require administration's immediate response with no time to obtain a warrant.[121] This "exigent circumstance" exception and probable cause definition amount to a standard. Judges consider the totality of circumstances after the fact to decide whether probable cause for the search existed and they decide whether a search was acceptable by consulting the defendant's reasonable expectation of privacy.[122] Instead of taking this ex post standard approach, what harm could be done in setting a rule that is uniform?

The judicial system seeks to both maximize social and economic well-being and minimize threats to inherent freedoms. By extension, the Fourth Amendment seeks to do the same, and in an economically efficient setting, it would minimize threats to privacy and any negative implications of the amendment. Economically speaking, the social and economic benefits that the law seeks to maximize are efficiency of the criminal justice system, control of

---

[121] *Probable Cause,* LEGAL INFORMATION INSTITUTE: CORNELL UNIVERSITY LAW SCHOOL, http://www.law.cornell.edu/wex/probable_cause (last visited May 14, 2014).

[122] *See* Ric Simmons, *Ending the Zero-Sum Game: How to Increase the Productivity of the Fourth Amendment,* 36 HARV. J. L. & PUB. POL'Y 549, 549 (2013).

crime, and in regards to the Fourth Amendment, to uphold overarching privacy rights. The negative implications and costs the law seeks to minimize include, but are not limited to, infringement of rights, judicial and administrative monetary costs, and the inefficiency of crime control and potential incompetence in the judicial and administrative system. Using a cost benefit analysis can depict the economics behind the Fourth Amendment and show how instituting a rule will maximize the economic efficiency of the law.

Professor Craig Lerner developed a formula along this reasoning to determine whether there is probable cause in a particular case.[123] Lerner adapts the Hand Formula from tort law to the context of a Fourth Amendment argument and proposes that a search would be reasonable if the social cost of the search in terms of the invasion of privacy is less than the social benefit of the search multiplied by the probability of the search being successful.[124] Said in different terms, if the social and economic benefits are greater than the costs, then the search is reasonable and probable cause exists. Learner emphasizes the importance of understanding the potential damages of the improper use of the Fourth Amendment and of maximization of the efficiency of searches that do occur when they are necessary. This economic analysis would not be the police officer's very first thought when making a split-second decision of whether or not he is justified to search or seize evidence a suspecting person. However, with a clear rule in place that sets a definite guideline for officers to abide by, the law and the actions acceptable under the law would be automatic.

The paradox of probable cause is that, in prescribing that measure, the original authors of the Constitution were binding us to a standard that itself could adapt to changed circumstances. Since the concept of probable cause has evolved since the Constitution's creation, the writers

---

[123] Craig S. Lerner, *The Reasonableness of Probable Cause*, 81 TEX. L. REV. 951, 1014-25 (2003).
[124] Simmons, *supra* note 9 at 555.

themselves may not have even had a clear idea of the specific meaning of that term. Thus, as it is today, the concept of probable cause is flexible – too flexible.[125] Realigning the probable cause standard into a taught rule based on this cost-benefit analysis will stabilize the core of Fourth Amendment precedent and further maximize social and economic benefits – accommodating law enforcement priorities while still preserving civil liberties on the other.

"... [A]nd particularly describing the place to be searched, and the persons or things to be seized."

One morning in Cleveland, Ohio in the late 1950s, police searched Ms. Dollree Mapp's home. They had acted on an anonymous tip and pretended to have a warrant. In this search, they found evidence that would emphasize the magnitude of Ms. Mapp's guilt. This case, Mapp v. Ohio, laid the foundation for the exclusionary rule with the Supreme Court's decision to ensure that unlawfully seized evidence would be excluded from state criminal trials.[126] To say that the exclusionary rule has been greatly debated would be an understatement. Justice Potter Stewart stated, "The exclusionary rule seems a bit jerry-built – like a roller coaster track constructed while the roller coaster sped along. Each new piece of track was attached hastily and imperfectly to the one before it, just in time to prevent the roller coaster from crashing, but without the opportunity to measure the curves and dips preceding it, or to contemplate the twists and turns that inevitably lay ahead."[127] But unless the exclusionary rule actually comes to be adjudicated as an ex ante rule, the roller coaster will run off of its track.

Researchers question whether the exclusionary rule deters police misconduct, whether imposition of the rule results in lost convictions, and whether it contributes to greater knowledge of the search and seizure law. This research amounts to the economic implications of the rule,

---

[125] *See* Lerner, *supra* note 12.
[126] CAROLYN N. LONG, MAPP V. OHIO: GUARDING AGAINST UNREASONABLE SEARCHES AND SEIZURES (2006).
[127] *Id.*

and its effectiveness on maximizing social and economic benefits. In a study conducted in 1974, researchers analyzed multiple cities to see the effects of the exclusionary rule and the Fourth Amendment.[128] The 1974 study "scrutinized motions to suppress evidence in narcotics, gambling, and weapons cases, as well as cases involving the possession and receipt of stolen property … in nineteen cities over a ten year period." The study concluded that the exclusionary rule's impact "depended much on such factors as degree of professional training prevailing in a department, policies of chiefs of police … and the attitude of mayors, city councils, and other officials, etc." There are many different constants and variables that go into each study; however, this particular research analyzed the effect of the suppression of evidence and the results concluded that administrative authorities should institute proper guidelines and policies of which the police and other authorizes should abide. Essentially, creating an ex ante rule would in effect make the Fourth Amendment law and the exclusionary rule most efficient.

It seems as though there is no Fourth Amendment norm, and thus no reliable source of uniformity. Yet, it would be in the best interests of the people to set a precedent rule that moves forward with an evolving and changing society while still holding static and textual consistency. The task of defining the rule of Fourth Amendment law should not be based on competing values and opinions of individual judges, but rather the meaning and scope should be clearly defined. This comment on the Fourth Amendment and the economic implications of the law is meant to be a simple introduction to the divergent opinions of the Fourth Amendment and its implications; it seeks to reason simple logical solutions to perpetually complex legal theory. In studying these opinions, conciliatory solutions can be made only if the entire judicial system reasons the same way, which in all actuality is contradictory of the federal republic system of the United States created by the Constitution. However, based on theory and evidence, an ex-ante, forward looking

[128] *Id.*

rule to adjudication under a living Constitution theory can establish judicial precedent to maximize the economic efficiency of the law, which will promote social and economic well-being in its Constitutional state.

LOCKEAN PRIVACY AND THE COURTS: AN AVENUE FOR LGBT RIGHTS IN AMERICA

Jesse Doggendorf

Abstract

In the United States, minorities consistently attempt to have their rights recognized within the Courts. One of these minorities, the LGBT community, has fought their specific type of oppression through different legal arguments – ranging from individual liberty guarantees to the condemnation of moral legislation. The variety of arguments and legal issues within LGBT cases has led to disagreements concerning the usefulness of each approach in obtaining the desired outcomes. I argue that the most successful and pragmatic route to equal rights for this community lies in the privacy arguments which have proven successful in the past. More specifically, advocacy for LGBT plaintiffs should be based in Lockean ideals concerning privacy. These ideals, properly understood, construct an umbrella under which the LGBT community may expect substantial progress in governmental recognition of its rights without negatively affecting their interests in equality.

Introduction

On June 26th, 2013, the United States Supreme Court announced a decision in the matter of *Windsor v. United States*. The Lesbian, Gay, Bisexual, and Transgender Community rejoiced at the Court's decision, which found the third section of the Defense of Marriage Act unconstitutional. By striking down DOMA's definition of marriage as a, "legal union between one man and one woman,"[129] the Court recognized the right of those within that community to be married before the federal government. This decision has also ushered in a new era of extensive LGBT litigation.[130] While scholars have discussed past LGBT-related decisions and the arguments used by both the litigants and the Court in said decisions, scholars have not discussed the usefulness of these same arguments in light of the Court's decision in *Windsor.* It is the purpose of this paper to examine the influence of the legal arguments endorsed by these scholars

[129] Defense of Marriage Act ("DOMA"), 1 U.S.C. § 7 (2006) and 28 U.S.C. §1738C (2006).
[130] Lila Shapiro, *Marriage Equality Lawsuits After DOMA Arise In South, Midwest, As Gay Rights Groups Urge Caution*, HUFFINGTON POST (July 31, 2013) http://www.huffingtonpost.com/2013/07/31/ marriage-lawsuits-doma.

in light of *Windsor* and to expand upon the argument that has been most persuasive in order to offer a more advantageous argument for future LGBT litigants. Specifically, this work will endorse privacy-based legal arguments, as they have been most influential on the Court in the past, and will advise that these arguments should be grounded in Lockean ideals, as some have been in the past, to ensure substantial progress for the LGBT community.

This paper will be divided into three sections. The first section of this work will focus on the question: *What legal arguments do scholars believe have worked in the past?* Previously, scholars have discussed the legal arguments used in cases concerning queer rights. Scholars have debated the legitimacy, thought processes behind, and success rates of different legal arguments used by LGBT litigants before *Windsor.* Most of these articles were written in the aftermath of *Lawrence v. Texas,* the case in which the United States Supreme Court ruled that state sodomy laws prohibiting same-sex intercourse were unconstitutional. By examining these articles, one may separate the scholars into contrasting schools of thought.

There are two schools of thought within the literature: one that is against using the privacy argument and one that advocates the use of the privacy argument. This work will present the first school of thought, composed of scholars who are against using the privacy argument, in two separate factions. The first faction in this school believes that the privacy argument only serves to undermine the LGBT community's ideals concerning equality. This faction's solution, using a rational basis argument, will then be addressed. The second faction in the first school believes that arguments that focus on 'liberty," not privacy, have been and would be more successful at obtaining favorable results for LGBT litigants. The second school of thought advocates for the continued use of the privacy argument. Finally, this section will conclude with a brief explanation of why the second school of thought is more persuasive.

The next section will address the question: *Which of the legal arguments above have previously proved significant in obtaining favorable outcomes in LGBT cases?* This section will dissect the privacy-based legal arguments used by the Court in LGBT-related cases, including *Bowers v. Hardwick* (1986) and *Lawrence v. Texas* (2003). Most important, the case of *Windsor v. United States* (2013), which has not been previously addressed in the contextual scholarly literature, will be discussed. In order to understand why privacy-based legal arguments proved most influential on the Court, the language and arguments in each of the opinions will be examined. The implications of *Windsor,* analyzed collectively with *Bowers* and *Hardwick*, allow one to conclude that a certain understanding of privacy-based legal arguments is most significant in obtaining favorable outcomes in LGBT-related cases.

Having addressed why I believe the privacy argument has proven most persuasive in the past, this work will proceed to the question: *How can the LGBT movement obtain favorable outcomes in the future?* I will begin this section with a brief analysis of Lockean ideals concerning privacy in order to show that the Court's understanding of an individual's right to privacy (especially in LGBT related cases) is rooted in these Lockean ideals. I further contend that, if the LGBT community is to succeed in their litigation endeavors, they must adhere to and expand upon the Court's Lockean-based understanding of an individual's right to privacy. Finally, I will respond to the criticisms of those scholars who are against using the right to privacy approach in LGBT cases in the context of this endorsed Lockean-based privacy argument.

I. Destroying the Wall: Differing Views on Influential Precedent in Past LGBT Cases

A. Problems With Privacy & The Alternatives

In the first school of thought, scholars speak against the "right to privacy" approach taken in past litigation. The first faction in this school believes that the privacy argument serves to undermine ideals concerning equality and does not encompass or guarantee the rights LGBT litigants are attempting to obtain. In his work *Repudiating Morals Legislation: Rendering the Constitutional Right to Privacy Obsolete,* Sonu Bedi claims that the privacy argument should be abandoned in light of the Court's decision in *Lawrence v. Texas.*[131] Bedi claims that the use of this legal principle is "not only problematic," but also has little support within the Constitution itself [132] and creates a discriminatory condition of "tolerance" when discussing LGBT rights.[133] "Tolerance" perpetuates that idea that the Court is allowing behaviors that they do not agree with and, by doing so, they condemn the LGBT community. This notion of tolerance, many scholars agree, is also problematic, as it serves to contrast homosexual and heterosexual relationships – labeling heterosexuals as "normal" and homosexuals as "the other." The application of the right to privacy in LGBT cases, these scholars argue, allows the state to degrade homosexual relationships as "deviant." [134] The Court, by only tolerating homosexuality in private, "has implicitly labeled [their] 'life-style' abnormal and shameful."[135] By arguing for LGBT rights under the legal principle of privacy, then, a precedent is created which "renders certain normative heterosexual couples as [the precedent's] primary reference point."[136] Therefore, homosexual relationships are treated just as heterosexual relationships are only to the extent that they are similar to heterosexuals.[137] Tolerance, then, labels LGBT individuals unequal before the

---

[131] Sonu Bedi, *Repudiating Morals Legislation: Rendering the Constitutional Right to Privacy Obsolete* 53 CLEV. ST. L. REV. 447, 447 (2006). *Lawrence v. Texas*, again, is the case in which the Supreme Court declared state sodomy laws that prohibited same sex intercourse unconstitutional. Lawrence v. Texas, 539 U.S. 538 (2002).
[132] *Id.* at 448.
[133] *Id.* at 449.
[134] *Id.* at 449.
[135] *Id.* 451.
[136] Katherine M. Franke, *The Domesticated Liberty of Lawrence v. Texas*, 104 COLUM. L. REV. 1399, 1415 (2004).
[137] *Id.* at 1419.

law. Lior Strahilevitz, another scholar, blatantly summarizes this flaw by stating: "Privacy protections create winners and losers."[138]

In this faction, there are also those who oppose using the right to privacy to support LGBT legal claims for different reasons. In the article *The Domesticated Liberty of Lawrence v. Texas,* Katherine M. Franke argues that the unwanted effects in privacy related positions on the LGBT community are not limited to ideals of "tolerance," but also in the "domesticated liberty" precedent creates. Franke states: "The Court relies on a narrow version of liberty that is both geographized and domesticated – not a robust conception of sexual freedom or liberty, as is commonly assumed."[139] By allowing this narrow view of liberty, the Court only allows LGBT citizens their liberties in the home and labels them unequal in the public sphere. Franke also claims that, in *Lawrence,* the Court "brings to bear a form of liberty that favors 'respect for [gay men's] private lives,' over 'the right to one's own concept of existence, of meaning, of the universe, and of the mystery of human life'."[140] By setting privacy precedents dependent upon an individual's identification with the LGBT community, many believe that a domesticated and narrow sense of liberty will evolve – leading to unfavorable future results in cases concerning more public matters. There is already evidence of this effect. In an article written by Anita L. Allen, Allen claims that this narrow approach to liberty has rendered privacy arguments useless in obtaining favorable outcomes for LGBT litigants in a large variety of cases, because said cases concern rights which are more public in nature (i.e. same sex marriage or employment discrimination).[141]The aforementioned consequences have convinced those within this faction to

---

[138] Lior Jacob Strahilevitz, *Toward a Positive Theory of Privacy Law*, 126 HARV. L. REV. 2010, 2010 (2013).
[139] Franke, *supra* note 136 at 1400.
[140] *Id.* at 1404. It is important to note that the first Court quotation comes from Kennedy's opinion in *Lawrence* and the second is from *Planned Parenthood v. Casey,* a privacy case unrelated to the LGBT community.
[141] Anita L. Allen, *Privacy Torts: Unreliable Remedies for LGBT Plaintiffs*, 98 CALIF. L. REV. 1711-12 (2010).

abandon arguments concerning privacy for those they feel more adequately address the needs of the community.

Only one of the previously mentioned scholars in this first faction has explicitly endorsed an alternative to the privacy argument for litigants in the LGBT community. Sonu Bedi encourages liberals to, "stick with a conception of rational review that prohibits appeal to mere morality."[142] Through a rational review argument, an individual may argue that restrictions on their liberties are irrational, as they serve no legitimate state interest. Bedi claims that such a rational review standard was constructed in the Supreme Court's decision in *Lawrence* (although it is not entirely prominent), and that the Court would recognize this precedent as a legitimate avenue for LGBT individuals to have their rights recognized.[143] Further, this author claims that the repudiation of moral legislation, "at the very least… secures the liberty we previously and problematically protected via the right to privacy."[144] Therefore, Bedi advocates rational review centered rhetoric in order to obtain favorable outcomes without the disparaging side effects of "tolerance" or "domesticated liberty" mentioned by him and others within the faction. I believe it is likely that other scholars within this faction would agree to use this type of legal argument, as it addresses their concerns.

The second faction in the anti-privacy school of thought claims that legal precedents concerning liberty were the most influential in past decisions and, therefore, would be the most practical for promoting equality for the LGBT community in the future. In his article *Justice Kennedy's Libertarian Revolution: Lawrence v. Texas*, Randy E. Barnett argues that the Supreme Court, in its decision to strike down state sodomy laws, was focused on protecting

---

[142] Bedi, *supra* note 131 at 448. Under a rational review standard, the government is required to show that a restriction on an individual's liberties serves a "legitimate" state interest and does not include questions of morality.
[143] *Id.* at 462.
[144] *Id.* at 454.

"liberty" rather than an individual's right to privacy.[145] The right to privacy, Barnett claims, is an insubstantial part of the Court's opinion and he insists that the majority opinion relies heavily on a "presumption of Constitutionality" for cases involving "fundamental rights."[146] Barnett states: "Justice Kennedy… is employing what I have called a 'presumption of liberty' that requires the government to justify its restriction on liberty, instead of placing the burden on the citizen by requiring the citizen to establish that the liberty being exercised is somehow 'fundamental.'"[147] Representing "nothing short of a Constitutional revolution," the author states that Justice Kennedy's opinion created ideals of "personal liberty," unbound by the "private zone" liberty restrictions placed on a citizen's right to privacy.[148] Barnett and those within this faction contend that an individual's right to privacy only exists under this overarching view of liberty set up by Kennedy in *Lawrence.* Other scholars agree with Barnett's anti-privacy focused conclusion and, what they consider to be *Lawrence's* "liberty" focused precedent. This factions' recommendation for future cases, one could assume, would focus on exploiting the government's inability to legitimately restrict LGBT citizens' personal liberties – an argument which they believe will guarantee more favorable outcomes.[149]

The rational review strategy endorsed by Bedi and this "liberty" focused analysis by Barnett are the only two alternatives to privacy clearly mentioned by scholars in this school of thought. Those within this school may feel that these solutions would be an adequate way to ensure favorable results in the future uncharacterized by the negative consequences of arguing an inherent right to privacy.

---

[145] Randy E. Barnett, *Justice Kennedy's Libertarian Revolution: Lawrence v. Texas*, 2003 CATO SUP. CT. REV. 21, 21 (2003). *See also* Arthur S. Leonard, *Lawrence v. Texas and the New Law of Gay Rights*, 30 OHIO N. U. L. REV. 189 (2004).
[146] Barnett, *supra* note 145 at 21.
[147] *Id.* at 36.
[148] *Id.* at 21.
[149] *Id.* at 36.

B. The Privacy Argument

The next school of thought includes those scholars who advocate for the continued use of the privacy argument in LGBT litigation efforts. In his article *Gay-Rights as a Particular Instantiation of Human Rights,* Vincent J. Samar argues that the equal protection clause allows "privacy interpreted in the right sense… to be protected."[150] Samar claims that the Supreme Court, in *Lawrence v. Texas*, was most interested in protecting individual liberty and, therefore, it chose an overarching legal principle (privacy) which "guarantees autonomy by providing individuals with the opportunity to perform private acts."[151]* Some believe that this inherent right to privacy, created in natural law, is the very foundation for all of our legal rights – separating us from a public sphere of control to a private sphere of freedom. Further, by acknowledging the privacy rights of an LGBT individual in *Lawrence*, the Court has bestowed upon those in this community the virtue of being human and deemed privacy advantageous avenue for future litigation.[152] By allowing an encompassing and expanding base of individual liberties, the Court promotes the use of privacy in future cases concerning diverse LGBT issues.

In his article *Liberty, Equality, and Privacy: Choosing a Legal Foundation for Gay Rights,* Richard A. Epstein argues that "privacy claims really involve a composite of claims that are based on the exercise of personal liberty."[153] Epstein is not the only scholar to believe that a citizen's right to privacy encompasses essential aspects of personal liberty. This understanding of the right to privacy most prominently protects an individual's "intimate decisions." Later in his article, Epstein lists "three facets of privacy," which offer a holistic view of this legal principle

---

[150] Vincent J. Samar, *Gay-Rights as a Particular Instantiation of Human Rights*, 64 ALB. L. REV. 983, 1009 (2001).
[151] *Id.* at 1014. It is import to note that this school's argument is the opposite of that used by scholars in the second faction of the first school, who believed that an overarching view of liberty encompassed an individual's right to privacy.
[152] R. Douglas Elliot & Mary Bonauto, *Sexual Orientation and Gender Identity in North America: Legal Trends, Legal Contrasts*, 48 JOURNAL OF HOMOSEXUALITY 94 (2005).
[153] Richard E. Epstein, *Liberty, Equality, and Privacy: Choosing a Legal Foundation for Gay Rights*, 2002 U. CHI. LEGAL F. 73, 96 (2002).

and allows one to answer whether the state may justify restrictions on the LGBT community underneath said principle.[154] First, the right to privacy creates places of greater liberty (labeled "zones") that, at the very least, protect consensual homosexual acts in private.[155] The scholar Wardenski also believes that these "zones," which privatize certain liberties, allows the LGBT community to claim that "sexual identity is a core part of human existence."[156] Wardenski believes this to be true, because the Court decided that homosexuality could not be Constitutionally prohibited in private and because the argument used, privacy, labels all that is protected by this legal principle an *essential liberty.*[157] The second facet in Epstein's work concludes that the state may only infringe upon an individual's privacy in favor of associated rights if there are threats to third parties.[158] The final component to this view of privacy is also the most important, concluding that the right to privacy protects the autonomy of the individual. Simply put, "individuals [under this principle] are entitled to 'freedom to choose how to conduct their lives'."[159] Understood in the context of *Lawrence,* this school of thought's view of privacy as a useful and effective tool in arguing for LGBT litigants in the Courts is most supported in the evidence, as I elaborate below.

The arguments which advocate using the right to privacy as a legitimate venue for LGBT equality are the most persuasive because past opinions have focused almost entirely on an individual's right to privacy and because it protects the autonomy of the individual. It now becomes important to ask: *How has the privacy argument worked well, and how can it be used in future litigation?* I wish to expand upon the concept of privacy and recommend a path for future

---

[154] *Id.*
[155] *Id.* at 97.
[156] Joseph J. Wardenski, *A Minor Exception?: The Impact of Lawrence v. Texas on LGBT Youth*, 95 NW. U. L. REV. 1410 (2005).
[157] *Id.*
[158] Epstein, *supra* note 153 at 98.
[159] *Id.*

litigants in this community. It is the main purpose of this work to argue that those fighting for LGBT equality in the Courts should use Lockean ideals to reshape privacy-based legal arguments, as it would assure the most favorable outcomes for future cases and encompass the rights the LGBT community is attempting to obtain without the previously mentioned negative consequences.

II. The Court's Privacy

This section of the work will dissect three of the most prevalent LGBT-related Court cases in the United States: *Bowers v. Hardwick* (1986), *Lawrence v. Texas* (2003), and *United States v. Windsor* (2013). It is abundantly clear, when reading these cases, that the privacy argument is the most debated legal principle by both the litigants and justices. By reading each opinion in sequential order, one may also see that the privacy argument has evolved to form a foundation that LGBT individual's liberties rest upon. While scholars have discussed the privacy argument's usefulness and implications on the LGBT community in the past, the case if *United States v. Windsor* has not been addressed in the scholarly discussion. In dissecting these cases, I will discuss language from the Court's opinions in order to assess which privacy-based arguments have proven most influential and useful in obtaining favorable outcomes for LGBT litigants. The discussions show how the Court has expanded ideals concerning privacy in order to incorporate the liberties and rights of LGBT individuals.

In 1986, the Supreme Court upheld state sodomy laws that prohibited same-sex intercourse in the case of *Bowers v. Hardwick.* Although the LGBT litigants in this case were unsuccessful in obtaining a favorable outcome, I believe both the majority and dissenting opinions offer insights into the Court's understanding of the privacy argument. In the majority opinion, Justice White stated that the right to privacy only protected those "fundamental

liberties," which are "deeply rooted in this Nation's history and traditions."[160] Along with their historical interpretation of what constitutes a fundamental liberty under the right to privacy, the majority also contended that previous privacy related precedents were attached to familial and free speech rights.[161] Because they concluded that neither of these rights are attached to homosexual sodomy, the majority upheld state sodomy laws that prohibited same-sex intercourse.[162] What is perhaps most telling, though, is that the majority spent its entire argument attempting to debunk the privacy-based legal reasoning of the LGBT litigants. Although this is true, the most relevant and precedential arguments concerning privacy are established in the dissenting opinion written by Justice Blackmun. Relying on an overarching view of privacy, Blackmun stated that, "this case is about 'the most comprehensive of rights and the right most valued by civilized men,' namely, 'the right to be let alone.'"[163] The dissent also stated that the majority relied too much on moral judgments, and used the precedents outlined in *Roe v. Wade* to conclude that moral legislation could not impede upon an individual's right to privacy.[164] Further, the dissent concluded that the LGBT litigant's, "privacy and […] right to intimate association does not depend in any way on his sexual orientation." The dissent's opinion concludes by summarizing their ideals concerning an individual's right to privacy:

> Our cases have long recognized that the Constitution embodies a promise that a certain private sphere of individual liberty will be kept largely beyond the reach of government. […] We protect those rights [because] they form so central a part of an individual's life.

[160] Bowers v. Hardwick, 478 U.S. 186, 192 (1986).
[161] *Id.*
[162] It is important to note that Justice Powell, in a concurring opinion, stated that imposing prison sentences on the individuals found guilty of same-sex sodomy could create serious 8th Amendment issues. 478 U.S. at 197.
[163] Bowers v. Hardwick, 478 U.S. 186, 199 (1986).
[164] *Id.*

> [The] concept of privacy embodies the 'moral fact that a person belongs to himself and not others nor to society as a whole'.[165]

It is this overarching view of privacy, set up in Blackmun's dissent, that became most influential on future cases before the Court. It is important to note that this view, which focuses entirely on an individual's right to live their lives, allowed future LGBT litigants a foundation on which to claim their liberties and rights. Seventeen years elapsed before the Supreme Court would hear another case concerning sodomy laws that prohibited same-sex intercourse.

In the case of *Lawrence v. Texas*, the Supreme Court struck down state sodomy laws that prohibited same-sex intercourse. Justice Kennedy, delivering the opinion of the Court, stated: "*Bowers* was not correct when it was decided, and it is not correct today. It ought not to remain binding precedent. *Bowers v. Hardwick* should be and now is overruled."[166] The majority opinion, not surprisingly, mirrors Blackmun's dissent in *Bowers* and focused on ideals concerning an individual's autonomy promised by the right their privacy. Justice Kennedy states: "It is the promise of the Constitution that there is a realm of personal liberty which the government may not enter."[167] This "realm" is the same "private sphere" mentioned in Blackmun's dissent in *Bowers*. It is this understanding of privacy that led the Court to conclude that, "The State cannot demean a homosexual person's existence or control their destiny" by making their private conduct a crime.[168] These statutes, the Court declared, attempt to control individual's behaviors, "in the most private of places, the home. These statutes seek to control a personal relationship that […] is within the liberty of persons to choose." [169] Justice Kennedy further expanded an individual's right to privacy in these statements. By expanding upon and

---

[165] *Id.* at 203.
[166] Lawrence v. Texas, 539 U.S. 558, 578 (2003).
[167] *Id.* at 578.
[168] *Id.*
[169] *Id.* at 558.

explaining Blackmun's "private sphere," the Court concluded that privacy not only protected sexual acts; it protected relationships between homosexual individuals and the right for all within the community to "choose their destiny." A LGBT individual's autonomy was, and still is, grounded in this overarching privacy foundation which protects their liberties. In his dissent, Scalia claimed that the majority's reasoning would "have far reaching implications beyond this case."[170] He was right.

In 2013, the case of *United States v. Windsor* was decided by the Supreme Court. Edith Windsor had sued the United States, claiming that Section 3 of the Defense of Marriage Act, which defined marriage as a legal union between one man and one woman, was unconstitutional because it violated her Fifth Amendment right to due process. The Court agreed. Relying on the precedent from *Lawrence*, Justice Kennedy (again delivering the opinion of the Court) once more expanded the privacy argument. In his opinion, Kennedy states that *Lawrence* protected one of many "[elements] in a personal bond that is more enduring."[171] Because the Court believed marriage has private implications and interferes with the ability of same-sex couples to have a family (perhaps the most important entity protected by the right to privacy), they ruled that the federal government must acknowledge same-sex marriages.[172] In this case, a LGBT individual's right to privacy was expanded to protect an individual's liberties that were both public and private in nature. Because an LGBT individual's right to privacy ensured and protected their liberties, the Court was able to rule Section 3 of DOMA unconstitutional "as a deprivation of the liberty of the person protected by the Fifth Amendment of the U.S. Constitution."[173] It is important to note that without the privacy-based foundation the liberties of

[170] Lawrence v. Texas, 539 U.S. 558, 586 (2003) (Scalia, J., dissenting).
[171] United States v. Windsor, 133 S. Ct. 2675, 2692 (2013).
[172] *Id.* at 2696.
[173] *Id.* at 2695.

LGBT individuals (including the right to marry) would not have been acknowledged and, therefore, could not have been protected.

While it is obvious that the privacy argument has played an influential role on the Court in LGBT-related cases, the evolution of the argument may not be as noticeable. Blackmun set a privacy-based foundation which promoted the protection of LGBT individual's rights in a specific sphere, which was then expanded by Kennedy in *Lawrence* to emphasize the autonomy of the individual and overturn *Bowers.* Finally, Kennedy expanded the argument even further to ensure that even the semi-public rights and liberties of LGBT individuals were protected under the Constitution. This evolution also allows one to understand which ideals concerning privacy have been most persuasive on the Court.

III. Lockean Privacy Ideals and LGBT Litigation

In this section, I contend that future LGBT litigation efforts must be grounded in Lockean ideals concerning privacy. These ideals have already proven influential on the Court and allow an avenue for substantial progress without undermining the LGBT community's devotion to equality.

In order to understand how Lockean ideals concerning privacy have influenced the Court in the cases above, it becomes necessary to briefly discuss Locke's views on privacy. In his *Second Treatise of Government,* Locke contends that the family was the first society and that it existed in a private state of nature.[174] In this natural state, individuals have complete autonomy over themselves and may form private societal connections.[175] Although this is true, Locke concludes that public political societies are still needed to protect the original autonomy and

[174] JOHN LOCK, SECOND TREATISE OF CIVIL GOVERNMENT §§ 77-83 (1690).
[175] *Id.* at § 81.

liberty of an individual in the private state of nature.[176] Individuals enter into a public political society by giving up their rights to execute the law of nature while also retaining their natural rights.[177] Because the public political society's purpose is to protect the individual's autonomy and liberty in private, a government may not intrude in the private sphere without providing a legitimate and significant state interest. Lockean ideology, then, establishes a clear line between the public political sphere and the private sphere it is created to protect. Because the Court recognizes these principles that lay at the foundation of our democracy, the privacy-based legal reasoning used by the justices mirror that of this Lockean ideology. This is especially true in LGBT related Court cases.

In Blackmun's dissent in *Bowers*, he contended that "the Constitution embodies a promise that a certain *private sphere* of individual liberty will be kept largely beyond the reach of government."[178] Lockean principles concerning the purpose of the public sphere and its separation from the private sphere are exemplified in this statement. Blackmun goes on to state: "[The] concept of privacy embodies the 'moral fact that a person belongs to himself and not others nor to political society as a whole.'"[179] Like Locke, Blackmun understands that the private sphere protects the autonomy and liberty of the individual. Lockean-like ideals also proved influential in the Court's decisions in *Lawrence* and *Windsor.* In *Lawrence,* Justice Kennedy again mentioned a "realm of personal liberty which the government may not enter."[180] This "realm" is Locke's private sphere. Further, Kennedy mentions that the state may not "control" a LGBT individual's destiny by "control[ing] a personal relationship."[181] These arguments mimic

[176] *Id.* at § 87.
[177] *Id.*
[178] 478 U.S. at 203 (Blackmun, J., dissenting) (emphasis added).
[179] *Id.* at 204.
[180] 539 U.S. at 578.
[181] *Id.* at 567.

Lockean privacy ideals concerning the autonomy of the individual and the individual's right to make private societal connections. Because these Lockean-grounded privacy arguments proved influential, the Court overruled its decision in *Bowers* and set an overarching privacy precedent for *Windsor*. Expanding on past precedent, the Court in *Windsor* ruled that the right to privacy encompassed personal bonds and the familial rights of an individual.[182] This correlates very closely with Lockean views on privacy and its foundation in the family. By rooting their reasoning in Lockean privacy ideals the Court has expanded an individual's right to privacy in these decisions.

Those arguments which mirror Lockean ideals concerning privacy have proven most beneficial in obtaining favorable outcomes for LGBT litigants in the past. In order to ensure substantial progress in the future, the LGBT community needs to continue framing their legal arguments in these principles. Further, those who advocate for LGBT rights in the Courts need to continue expanding upon these principles by arguing for Locke's overarching view of privacy. By doing so, these arguments may create an umbrella to fight for and keep safe those liberties LGBT individuals still struggle to obtain.

Many of the previously mentioned concerns of those scholars in the first school can be addressed by using Lockean ideals to construct an overarching view of privacy in future cases. First, the right to privacy understood in Lockean terms would not promote ideals of "tolerance," as the right to privacy would apply to all individuals independent of their sexual orientation.[183] Further, because Lockean privacy ideals create a foundation that encompasses all individual liberties, protecting certain liberties under the right to privacy would not degrade these liberties by labeling them "tolerable." If the privacy argument is framed in Lockean ideals, the liberties

[182] *See* United States v. Windsor, 133 S. Ct. 2675 (2013).
[183] See the above discussion over Blackmun's dissent in *Bowers*, in which he stated: "privacy and […] the right to intimate association does not depend in any way on his sexual orientation." 478 U.S. at 201.

protected by privacy would not be domesticated, as the right to privacy would encompass liberties both inside and outside of the home. That a Lockean view of privacy would not domesticate liberties is already evidenced by the Court's decision in *Windsor*. Privacy arguments framed in Lockean ideals would not only allow substantial progress in LGBT litigation, but also address the previous concerns of scholars in the field.

Conclusion

Before the Court's decision in *Windsor*, there were conflicting views on the usefulness of the privacy argument in LGBT related Court cases. While some contended that arguing for an LGBT individual's right to privacy did not guarantee favorable outcomes, others claimed that the use of the privacy argument had harmful side effects on the community's struggle for equality. Nonetheless, the privacy argument has proved most persuasive in past Court decisions. The legal reasoning of the Court in these past cases mirrors Lockean ideals concerning privacy and the autonomy of the individual in the private sphere. Using Lockean-based privacy arguments would also address the concerns of previous scholars. Therefore, I advise LGBT litigants to ground privacy arguments in Lockean ideals in order to ensure substantial progress for their community.

In this paper, I have carefully tailored the right to privacy for the queer community specifically and acknowledge that many concerns of Feminist Scholars are not addressed. In light of these concerns, I only endorse the privacy argument to protect individual liberties so long as it does not threaten third parties.[184] However, a further examination of this work's argument may prove useful in reshaping a privacy argument that would not be harmful to women. It is my belief that an appropriate understanding of an individual's right to privacy could have far reaching effects.

[184] See the above discussion concerning Epstein's work.