Golden Gate University Law Review

Volume 47 | Issue 2 Article 10

May 2017

Hackers Made Me Lose My Job!: Health Data Privacy and Its Potentially Devastating Effect on the LGBTQ Population

Alex Lemberg
Golden Gate University School of Law

COMMENT

HACKERS MADE ME LOSE MY JOB!: HEALTH DATA PRIVACY AND ITS POTENTIALLY DEVASTATING EFFECT ON THE LGBTQ POPULATION

*ALEX LEMBERG**

"The nature of injustice is that we may not always see it in our times."

–Justice Anthony Kennedy

INTRODUCTION

Your personal health records contain some of the most sensitive personal data about you, but your information might already be publicly available on the Internet. Healthcare records comprised two-thirds of all data targeted by computer hackers in 2015,[1] and hackers accessed 98% of all breached healthcare records.[2] Hackers illegally obtained over 112 million personal health records in the United States in 2015 — a number

* J.D. Candidate, May 2017, Golden Gate University School of Law; B.A. Geography, August 2011, University of California, Berkeley. I would like to thank Professor Mark Yates, Professor Laura Cisneros, and Magistrate Judge Laurel Beeler for reading my comment and providing thoughtful commentary and suggestions throughout my writing process. Thanks and deepest appreciation to my husband and my family for their love and support throughout this entire process. Thanks also to Mary Loung, Heather Varanini, and Cara Alsterberg, without whom this comment and this publication would not be possible.

[1] IDENTITY THEFT RES. CTR., ITRC DATA BREACH REPORTS 4 (Dec. 31, 2015), http://www.idtheftcenter.org/images/breach/DataBreachReports_2015.pdf.

[2] Fred Pennic, *Report: Hackers Caused 98% of Healthcare Breaches in 2015*, HIT CONSULTANT (Jan. 28, 2016), http://hitconsultant.net/2016/01/28/hackers-caused-98-of-healthcare-data-breaches/.

equivalent to over one third of the nation's population.[3] Hackers are smart; a health insurance credential on its own can net $20 on the black market,[4] a Medicare number can sell for up to $50,[5] and each set of health data records together with related counterfeit documents can potentially be sold for $1,300.[6] Even if only 10% of accessed health records include a Medicare number, sales of those numbers would amount to $5.6 billion. These astonishing numbers, largely driven by hackers who target large corporations,[7] exist alongside smaller but even more damaging data breaches.

In December 2015, hackers publicly leaked the personal information of 4,926 users of Hzone, a dating app for HIV-positive singles, including their names, sexual orientations, dates of birth, and email addresses, along with the inference that the users of this app were HIV-positive.[8]

Although hackers frequently steal private data for financial gain, they may also have more sinister intentions. Gay and bisexual men comprise 67% of all HIV-positive people in the United States[9] despite being only 2.2% of the overall population.[10] Hackers can easily make the connection that while HIV status is a protected class under federal laws against employment and public accommodations discrimination,[11] sexual orientation is not, and therefore any hint of an individual's sexual orientation can be used against the person. This points to additional potential rationales other than solely monetary gain, such as animus, hatred, and schadenfreude.

The intentional release of 37 million Ashley Madison[12] account holders' private information in July 2015 revealed the extent hackers are

---

[3] IDENTITY THEFT RES. CTR., *supra* note 1, at 4.

[4] Jeanine Skowronski, *What Your Information Is Worth on the Black Market*, BANKRATE.COM (July 27, 2015), http://www.bankrate.com/finance/credit/what-your-identity-is-worth-on-black-market.aspx.

[5] Reed Abelson & Matthew Goldstein, *Anthem Hacking Points to Security Vulnerability of Health Care Industry*, N.Y. TIMES (Feb. 5, 2015), http://www.nytimes.com/2015/02/06/business/experts-suspect-lax-security-left-anthem-vulnerable-to-hackers.html.

[6] Skowronski, *supra* note 4.

[7] Pennic, *supra* note 2.

[8] Jasper Hamill, *HIV Dating App HZone 'Leaks 5,000 People's Private Details' During Devastating Alleged Data Breach*, MIRROR (Dec. 16, 2015, 2:10 PM), http://www.mirror.co.uk/news/technology-science/technology/hiv-dating-app-hzone-leaks-7021486.

[9] Centers for Disease Control and Prevention, *HIV in the United States: At a Glance*, CDC.GOV, http://www.cdc.gov/hiv/statistics/overview/ataglance.html (last visited Feb. 7, 2017).

[10] BRIAN W. WARD, JAMES M. DAHLHAMER, ADENA M. GALINSKY & SARAH S. JOESTL, SEXUAL ORIENTATION AND HEALTH AMONG U.S. ADULTS: NATIONAL HEALTH INTERVIEW SURVEY, 2013 7 (Nat'l Health Statistics Reports No. 77, 2014), http://www.cdc.gov/nchs/data/nhsr/nhsr077.pdf.

[11] Nat'l Ass'n of Soc. Workers, *Discrimination & HIV/AIDS: A Factsheet for Practitioners,* http://www.naswdc.org/diversity/lgb/hiv_discrimination.asp (last visited Feb. 7, 2017).

[12] Ashley Madison is a website that, at the time of the breach in 2015, advertised itself primarily as a connection for married heterosexual people to conduct extramarital affairs. Its homepage in

willing to go to ruin people's lives.[13] A group of hackers, known only as "The Impact Team," intentionally breached Ashley Madison's user database[14] in order to embarrass, subject to public ridicule, and destroy the relationships of millions of people who joined the service seeking extramarital affairs.[15] Ashley Madison's parent company also operates a website called "Down Low," a term which generally refers to sexual practices of married, heterosexual-identifying men who have sex with other men.[16] The information of Down Low users was leaked along with the rest of the Ashley Madison user data.[17] The breach was made worse by the creation of websites where anyone could enter an email address to see if that address was associated with an Ashley Madison account.[18]

Because the vast majority of Ashley Madison users were heterosexual, only a few media outlets focused on the dire effects caused by the Ashley Madison breach on the lesbian, gay, bisexual, transgender, and queer ("LGBTQ") population. These sources presented stories that painted bleak pictures for gay men in countries like Saudi Arabia, where being caught participating in same-sex sexual activity is punishable by death.[19] Global News contrasted this outcome with the consequences faced by breach victims in the United States, who face "damaged or destroyed marriages, or the loss of a security clearance."[20] The consequences also included two suicides in Canada,[21] but the prospect of the death penalty for the possession of an account on a website is extreme.

2015 stated, "Ashley Madison is the most famous name in infidelity and married dating." Their infamous slogan was "Life is Short, Have an Affair." As of the time of this publication, Ashley Madison had rebranded itself as "the world's largest, most open-minded dating community."

See Kim Zetter, *Hackers Finally Post Stolen Ashley Madison Data*, WIRED (Aug. 18, 2015, 5:55 PM), https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/; ABOUT ASHLEY MOMENTS, https://blog.ashleymadison.com/about/ (last visited Feb. 4, 2017).

[13] Zetter, *supra* note 12.

[14] *See* Associated Press, *Two Suicides Linked to Ashley Madison Breach*, N.Y. POST (Aug. 24, 2015, 11:51 AM), http://nypost.com/2015/08/24/two-suicides-linked-to-ashley-madison-leak/.

[15] *See* Jose Pagliery, *The Ashley Madison Hack Ruined My Life*, CNN MONEY (Aug. 21, 2015, 5:41 PM), http://money.cnn.com/2015/08/21/technology/ashley-madison-ruined-lives/.

[16] *See* Paul Gallagher, *Ashley Madison Hack: Leaking Personal Email Addresses Puts Gay Lives at Risk Around the World,* INDEPENDENT (Aug. 20, 2015), http://www.independent.co.uk/news/world/ashley-madison-hack-leaking-personal-email-addresses-puts-gay-lives-at-risk-around-the-world-10464546.html.

[17] *See id.*

[18] *Was Your Profile Compromised in the Ashley Madison Hack?*, https://ashley.cynic.al (last visited Feb. 7, 2017).

[19] *See* Patrick Cain, *Where 1,296 Gay Ashley Madison Users Face Prison, Flogging, Execution*, GLOBAL NEWS (Sept. 2, 2015, 10:18 AM), http://globalnews.ca/news/2186587/where-1296-gay-ashley-madison-users-face-prison-flogging-execution.

[20] *Id.*

[21] *See* Associated Press, *supra* note 14.

Although Ashley Madison users in the United States did not face the death penalty, the breach carried severe potential consequences for gay and bisexual men. Because of the leak from the Down Low site, the general public had full access to data that connected names of individuals with their sexual orientation. Anyone can easily search for any individual, who then may face discrimination due to the lack of legal protections for LGBTQ people in the United States.

The team of hackers behind the Ashley Madison breach believed the site to be morally wrong.[22] Personal definitions of morality greatly influence the minds of many Americans and cause people to discriminate against those they consider immoral.[23] The Impact Team expressed their intent before publishing the breached data: "[t]oo bad for those men, they're cheating dirtbags and deserve no such discretion."[24]

Moral wrongness has engrained itself into American civil rights legislation, as well. Only 22 states and the District of Columbia have enacted legislation protecting lesbian, gay, and bisexual individuals from discrimination in employment, housing, and public accommodations.[25] Only 19 states and the District of Columbia have those same full protections for transgender people.[26] In states without these protections, LGBTQ people can be fired, not hired, denied housing, evicted, or removed from retail establishments solely on account of their sexual orientation or gender identity. Therefore, data breaches like Ashley Madison, which publicly released names and information about sexual orientation or gender identity, pose a grave threat of discrimination to millions of LGBTQ Americans.

Although there has not yet been a reported case of discrimination that has been explicitly linked to breached health information, the potential for future discrimination, driven by animus, is limitless. This may seem to be a mere hypothetical considering the lack of concrete examples, but actual human beings' jobs, homes, and safety are at risk as shown by the response and backlash from the recent advancements in LGBTQ rights.

---

[22] IMPACT TEAM MANIFESTO, http://pastebin.com/3SepJr8Q (last visited Feb. 4, 2017).

[23] Jennifer Stuber, Ilan Meyer & Bruce Link, Stigma, Prejudice, Discrimination and Health 6 (2008) (unpublished manuscript) (on file with Pub Med Central, National Institute of Health), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4006697/pdf/nihms338971.pdf (published at 67 SOC. SCI. MED. 351 (2008)) (discussing that being viewed by society as immoral lessens social capital).

[24] Alyssa Newcomb, *Ashley Madison Hack: What We Know About the Group Behind It*, ABC NEWS (Aug. 20, 2015, 3:42 PM), http://abcnews.go.com/Technology/ashley-madison-hack-group/story?id=33210317.

[25] *See* Non-Discrimination Laws: State by State Information – Map, AM. CIVIL LIBERTIES UNION, https://www.aclu.org/map/non-discrimination-laws-state-state-information-map (last visited Feb. 4, 2017).

[26] *Id.*

This Comment shows that because of an increasing rate and severity of data breaches, insufficient legal recourse for affected individuals, and lack of incentives for healthcare companies to strengthen their data security systems, leaked healthcare data will cause the substantive due process right of privacy of LGBTQ individuals to be disenfranchised. Because sexual orientation and gender identity are unprotected by heightened scrutiny under federal due process and equal protection jurisprudence, additional protections must be created for LGBTQ people. These protections should include a new legal right in tort under the Health Information Portability and Accountability Act of 1996 (HIPAA), increase incentives for protecting electronic health data, and increase budget to fund enforcement and compliance activities.

Part I-A of this Comment includes a brief background of sexual orientation and gender identity anti-discrimination laws at the federal and state levels, and the injuries that occur when the laws do not exist. Part I-B provides an overview of the current laws that protect a patient's right to privacy, including HIPAA, the Health Information Technology for Economic and Clinical Health Act (HITECH), and the Patient Protection and Affordable Care Act (ACA). Emphasis will be placed on healthcare needs specific to the LGBTQ population and why that has led to a push for sexual orientation and gender identity information being collected from patients and remedies for breach victims. Part II argues that the results of health data breaches will lead to discrimination and the suppression of substantive due process rights of LGBTQ individuals. Part II will also provide a comprehensive legislative and regulatory plan as well as judicial suggestions to both prevent future data breaches and provide the LGBTQ population additional avenues of remedy. Part III concludes by considering the implications of these suggested changes.

I. BACKGROUND

In order to understand the need for stronger protections against data breaches and hacking to protect LGBTQ people, the development of over 50 years of anti-discrimination laws and over 20 years of health data privacy laws must be reviewed. A basic understanding of these laws is paramount to implementing change. This section reviews civil rights legislation in the United States at the federal and state levels, notes modern trends in those substantive protections, discusses injuries when sufficient protections do not exist, and explains the federal scheme of health data protection laws.

A. FEDERAL AND STATE CIVIL RIGHTS LAWS PROTECTING LGBTQ PEOPLE

The legal scheme for protecting LGBTQ people in the United States is a complicated mash-up of mixed-motive laws, confusing Supreme Court and appellate court decisions, and conflicting executive actions. The most important legislation and regulations will be discussed in order to acquaint the reader with the tumultuous history of LGBTQ rights.

1. Federal Laws

One of the greatest legislative victories in Twentieth Century America was the passage of the Civil Rights Act of 1964. This landmark law banned discrimination on the grounds of race, color, religion, and national origin.[27] Specifically, Title II of the Civil Rights Act banned discrimination in public accommodations, such as hotels, restaurants, retail establishments, and entertainment facilities that engaged in interstate commerce.[28] Similarly, the Civil Rights Act's Title VII protected the same classes from discrimination in employment.[29] Four years later, Congress added protections against housing discrimination in Title VIII of the Civil Rights Act of 1968.[30] Fifty years have elapsed since the passage of the Civil Rights Act of 1964 and yet lesbians, gay men, bisexuals, transgender people, and queer people still do not have similar protections under federal law.

The fight for LGBTQ equality and civil rights began in earnest shortly after the passage of the Civil Rights Act of 1964. During the August 1966 Compton's Cafeteria riot in San Francisco, police raided a transgender gathering place in San Francisco's Tenderloin District, resulting in a riot.[31] The rioters became known as the "Screaming Queens" and provided the first glimpse of a major movement.[32] On June 28, 1969, the New York Police Department discriminatorily raided New York's

[27] *See* Civil Rights Act of 1964 § 201(a), 42 U.S.C. § 2000a(a) (2015).

[28] *See* Civil Rights Act of 1964 § 201(b), 42 U.S.C. § 2000a(b) (2015).

[29] *See* Civil Rights Act of 1964 § 703(a), 42 U.S.C. § 2000e-2(a) (2015).

[30] *See* Civil Rights Act of 1968 (Fair Housing Act) § 804, 42 U.S.C. § 3604 (2015).

[31] Ryan Kost, *The Riot that Predated Stonewall, 50 Years Later*, S.F. CHRON. (June 25, 2016), http://www.sfchronicle.com/bayarea/article/The-queer-riot-that-predated-Stonewall-50-years-8323730.php.

[32] Daniel Villarreal, *Before Stonewall, There Was the Cooper's Donuts and Compton's Cafeteria Riots*, QUEERTY (Oct. 7, 2011), https://www.queerty.com/before-stonewall-there-was-the-coopers-donuts-and-comptons-cafeteria-riots-20111007/2 (explaining that San Francisco's response to the riot was different from New York's reaction to Stonewall; the city created "[a] network of social, mental, and medical support services" including the "National Transsexual Counseling Unit, overseen by a member of the [San Francisco Police Department].").

most popular gay bar, the Stonewall Inn.[33] Although the police had raided the bar many times before, unrest grew that evening, and more gay men, lesbians, and trans and queer people joined the rebellion.[34] The Stonewall riot lasted for six days; its participants fought against laws and law enforcement that specifically targeted the closure of gay spaces.[35] The Stonewall riot was a major landmark in the LGBTQ rights movement, and one year later, the first gay pride celebrations were held simultaneously in New York, San Francisco, Los Angeles, and Chicago.[36] LGBTQ pride celebrations continue in many cities, including San Francisco, Chicago, Seattle, and New York, annually on the last weekend in June to commemorate Stonewall.[37] Both the Compton's Cafeteria riot and the Stonewall riot have been officially commemorated: the Stonewall Inn is now a National Monument[38] and the San Francisco Board of Supervisors will vote to approve a transgender historic district in the area around the former site of Compton's Cafeteria in 2017.[39]

On the five-year anniversary of the Stonewall riots, a bill was introduced to Congress that would have amended the Civil Rights Act of 1964 to prohibit discrimination in employment and public accommodations based on sex, marital status, or sexual orientation.[40] It was unsuccessful, but renamed the Employment Non-Discrimination Act (ENDA) and reintroduced in the House of Representatives in 1994.[41] Since then, ENDA has been reintroduced numerous times, but has failed each time;[42]

---

[33] Garance Franke-Ruta, *An Amazing 1969 Account of the Stonewall Uprising*, THE ATLANTIC (Jan. 24, 2013), https://www.theatlantic.com/politics/archive/2013/01/an-amazing-1969-account-of-the-stonewall-uprising/272467/.

[34] *Stonewall Riots: The Beginning of the LGBT Movement*, THE LEADERSHIP CONFERENCE (June 22, 2009), http://www.civilrights.org/archives/2009/06/449-stonewall.html.

[35] Franke-Ruta, *supra* note 33.

[36] THE LEADERSHIP CONFERENCE, *supra* note 34.

[37] Andrew Collins, *June Gay Pride Calendar 2017,* ABOUT TRAVEL (Nov. 30, 2016), http://gaytravel.about.com/od/gaypridefestivals/qt/GayPride_June.htm.

[38] Press Release, President Barack Obama, Presidential Proclamation – Establishment of the Stonewall National Monument (June 24, 2016), https://obamawhitehouse.archives.gov/the-press-office/2016/06/24/presidential-proclamation-establishment-stonewall-national-monument.

[39] Toshio Meronek, *San Francisco May Soon Have the World's First Transgender Cultural District*, VICE (Feb. 2, 2017, 2:57 PM), https://www.vice.com/en_us/article/san-francisco-may-soon-have-the-worlds-first-transgender-cultural-district.

[40] Equality Act, H.R. 14752, 93d Cong. (1974).

[41] Employment Non-Discrimination Act of 1994, H.R. 4636, 103d Cong. (1994).

[42] Leigh Ann Caldwell, *Sexual Orientation and Employment Nondiscrimination Act: How We Got Here*, CNN.COM (Nov. 4, 2013, 7:25 PM), http://www.cnn.com/2013/11/04/politics/employment-nondiscrimination-timeline/ (explaining forty years of history of ENDA and how partisan politics and earnest bipartisan efforts have changed the scope of the bill to be alternately inclusive and exclusive of transgender rights).

in line with recent obstructionist tactics, the Republican-controlled House most recently rejected it in December 2014.[43]

The executive branch recently extended new protections for LGBTQ individuals in the absence of legislative action. President Obama signed Executive Order 13672 in December 2014, which extended employment discrimination protections to LGBTQ people working as federal employees, contractors, or subcontractors.[44] Additionally, the Equal Employment Opportunity Commission ("EEOC") found in two separate appeals before administrative judges that discrimination against an individual because of sexual orientation and gender identity is sex discrimination under Title VII of the Civil Rights Act of 1964.[45] While this does, in theory, apply to all private employment, the EEOC's precedents are merely persuasive to federal courts hearing employment discrimination related cases.[46] Other areas, such as public accommodations, have no federal protections currently.[47] Simply stated, current federal laws do not sufficiently protect LGBTQ people from discrimination; without a willing Congress, LGBTQ people must rely on states to pass and enforce these laws. This lack of protection by federal laws will lead to data breach victims facing discrimination. In some cases, state laws can fill the gaps in federal protections, but many states still do not offer any protection at all.

2. State Laws

States vary drastically in regard to the amount of LGBTQ anti-discrimination protections offered under state law. The extreme ends of the spectrum are represented by California and Tennessee/North Carolina. California has some of the strongest protections in the United States for LGBTQ people, while Tennessee and North Carolina have passed laws to restrict liberty of LGBTQ individuals. This section shows the striking

---

[43] Chris Johnson, *House Panel Rejects Last-Ditch Effort to Pass ENDA*, WASH. BLADE (Dec. 3, 2014, 8:56 PM), http://www.washingtonblade.com/2014/12/03/house-panel-rejects-last-ditch-panel-pass-enda/.

[44] 41 C.F.R. § 60-1.4 (2015); Exec. Order No. 13672, 3 C.F.R. § 42971 (2014).

[45] *What You Should Know About EEOC and the Enforcement Protections for LGBT Workers*, U.S. EQUAL EMP'T OPPORTUNITY COMM'N, http://www.eeoc.gov/eeoc/newsroom/wysk/enforcement_protections_lgbt_workers.cfm (last visited Feb. 7, 2017).

[46] Dale Carpenter, *Anti-Gay Discrimination Is Sex Discrimination, Says the EEOC*, WASH. POST: VOLOKH CONSPIRACY (July 16, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/07/16/anti-gay-discrimination-is-sex-discrimination-says-the-eeoc/.

[47] *See* Civil Rights Act of 1964 § 201(a), 42 U.S.C. § 2000a(a) (2012) (stating that the only classifications protected from public accommodations discrimination are race, color, religion, and national origin).

contrast between the maximum and minimum protections offered between American jurisdictions.

a. California

California has full anti-discrimination protections under employment,[48] housing,[49] and public accommodations,[50] meaning that in all aspects of public life, LGBTQ people cannot be discriminated against and must receive the same benefits under California law as all other people. California residents have the right to bring civil suits for damages or equitable relief against violators of these laws, meaning they can file a lawsuit against anyone who takes their rights away in any fashion.[51]

California also has a history of leadership in passing progressive legislation. Currently, California allows transgender children to use the restrooms of their choice and play sports on teams that accord with their preferred gender identity.[52] California also prohibits LGBTQ-discriminatory education in public schools.[53]

Many municipalities within the state of California offer additional protections to LGBTQ people. For example, the City and County of San Francisco created a countywide agency called the Human Rights Commission, which began authoring legislation protecting transgender and gender nonconforming people in 1995.[54] The Human Rights Commission also has the power to investigate and mediate "community-wide problems . . . which may result in intergroup tensions or discrimination."[55]

b. Tennessee and North Carolina

It is a true test of federalism to compare local ordinances in San Francisco to laws in states such as Tennessee and North Carolina. Tennessee does not have any state employment, housing, or public accommodations protections for its LGBTQ residents, and the state went one step further by banning local anti-discrimination ordinances. The Ten-

[48] CAL. GOV'T CODE § 12940 (2015).

[49] *Id.* at § 12955 (2012).

[50] CAL. CIV. CODE § 51 (2012).

[51] *Id.* at § 52.1(b) (2015).

[52] CAL. EDUC. CODE § 221.5(f) (2015).

[53] *Id.* at §§ 51500–51501 (2013).

[54] *Compliance Guidelines to Prohibit Gender Identity Discrimination*, HUMAN RIGHTS COMM'N (Dec. 10, 2003), http://sf-hrc.org/compliance-guidelines-prohibit-gender-identity-discrimination.

[55] S.F., CAL., ADMIN. CODE § 12A.5(a) (2000), https://law.resource.org/pub/us/code/city/ca/SanFrancisco/Administrative%20Code/chapter12a.html.

nessee legislature passed the "Equal Access to Intrastate Commerce Act,"[56] which banned local anti-discrimination ordinances under the guise of being pro-business in response to the city of Nashville's local LGBTQ anti-discrimination ordinance.[57] Neighboring North Carolina recently passed a bill, HB 2, banning transgender people from using the bathrooms of their choice.[58] These two laws seemingly conflict with the Supreme Court's 1996 decision in *Romer v. Evans*, which invalidated a Colorado constitutional amendment that banned local LGB anti-discrimination ordinances because it violated the Equal Protection Clause of the Fourteenth Amendment.[59] The difference between the Colorado amendment in *Romer* and the laws in Tennessee and North Carolina is the focus — the Colorado amendment explicitly singled out LGBTQ people, while the Tennessee and North Carolina laws purported to protect local businesses from the economic burden of anti-discrimination laws.[60] The American Civil Liberties Union and other progressive organizations filed a lawsuit to repeal the North Carolina law.[61] The case is currently pending before the Fourth Circuit Court of Appeal, following a federal judge granting a partial preliminary injunction.[62]

Now more than ever, the fear of adding LGBTQ rights is being described as a religious moral issue. Franklin Graham, son of famous televangelist Billy Graham, stated on his website that HB 2 in North Carolina "isn't only an important issue of privacy and safety, this is a moral issue."[63] His bold statement shows the dangerous role religion may play in suppressing the rights of those they view differently, like the LGBTQ population.

Because of the wide variances between states with maximum protections and states that have legalized discrimination, differing levels of injuries due to discrimination are bound to occur. Far from only causing

---

[56] TENN. CODE ANN. § 7-51-1802 (2016).

[57] Lisa Keen, *Showdown Brewing over Tennessee Anti-Gay Law*, KEEN NEWS SERVICE (May 25, 2011), http://www.keennewsservice.com/201/05/25/showdown-brewing-over-tennessee-anti-gay-law/.

[58] H.B. 2, 2015-2016 Gen. Assemb., 2d Extra Sess. (N.C. 2016).

[59] Romer v. Evans, 517 U.S. 620, 635-36 (1996).

[60] Jeff Guo, *The Cunning Trick in North Carolina's Radical New Anti-LGBT Law*, WASH. POST: WONKBLOG (Apr. 1, 2016), https://www.washingtonpost.com/news/wonk/wp/2016/04/01/the-cunning-trick-in-north-carolinas-radical-new-anti-lgbt-law/.

[61] Complaint, Carcaño v. McCrory, No. 1:16-cv-236 (M.D.N.C. 2016), https://www.aclu.org/sites/default/files/field_document/dkt_1_-_carcano_v._mccrory_complaint.pdf.

[62] Carcaño v. McCrory, ____ F. Supp.3d ____, 2016 WL 4508192 (M.D.N.C. 2016), *appeal docketed* No. 16-1989 (4th Cir. filed Aug. 30, 2016).

[63] Decision Magazine, *Franklin Graham on N.C.'s HB2: "It's a Moral Issue"*, BILLYGRAHAM.ORG (Sept. 15, 2016), https://billygraham.org/story/franklin-graham-on-n-c-s-hb2-its-a-moral-issue-2/.

isolation and embarrassment in peoples' lives, discrimination has severe tangible physical and mental effects on those people who experience it.

B. INJURIES DUE TO DISCRIMINATION

There is a paucity of academic research on the actual effects of discrimination on the LGBTQ population as a whole, despite academics expending significant resources on researching specialized areas, such as impact on LGBT youth, employment discrimination, and mental health.[64] Health data breaches present a new and unwelcome way of releasing private sexual orientation data to the public, which could lead to greater levels of discrimination if it falls into the wrong hands. Some concrete findings regarding LGBTQ discrimination are presented below.

A Harvard researcher sent out 1,769 pairs of fictitious resumes to employers hiring entry-level employees for white-collar companies in seven states, which represent different regions of the United States.[65] The resumes sent in this study were identical, except for one line in one resume stating experience in a university campus LGBT group and the other omitting that line.[66] This study presents a sociological perspective that shows direct evidence of discrimination, as opposed to the effects of the discrimination as shown from the perspective of public health. The research showed that employment discrimination against gay men varied significantly between different regions of the United States, but overall,

---

[64] Vickie M. Mays & Susan D. Cochran, *Mental Health Correlates of Perceived Discrimination Among Lesbian, Gay, and Bisexual Adults in the United States*, 91 AM. J. PUB. HEALTH 1869, 1874 (2001), http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1446893/pdf/0911869.pdf (finding that increases in perceived discrimination by lesbian, gay, and bisexual people cause an increase in the incidence of physical and psychological deterioration with co-occurring psychological disorders); LAURA E. DURSO & GARY J. GATES, SERVING OUR YOUTH: FINDINGS FROM A NATIONAL SURVEY OF SERVICE PROVIDERS WORKING WITH LESBIAN, GAY, BISEXUAL, AND TRANSGENDER YOUTH WHO ARE HOMELESS OR AT RISK OF BECOMING HOMELESS 3-4 (The Williams Institute with True Colors Fund and The Palette Fund, eds. 2012), http://williamsinstitute.law.ucla.edu/wp-content/uploads/Durso-Gates-LGBT-Homeless-Youth-Survey-July-2012.pdf (finding that 40% of all homeless youth identify as LGBTQ and that the number one reason for youth homelessness in this population is family rejection); BRAD SEARS & CHRISTY MALLORY, DOCUMENTED EVIDENCE OF EMPLOYMENT DISCRIMINATION & ITS EFFECTS ON LGBT PEOPLE (The Williams Institute, ed. 2011), http://williamsinstitute.law.ucla.edu/wp-content/uploads/Sears-Mallory-Discrimination-July-20111.pdf (linking workplace discrimination with psychological distress, health problems, lower job satisfaction, and higher absenteeism); Gilbert Herdt & Robert Kertzner, *I Do, but I Can't: The Impact of Marriage Denial on the Mental Health and Sexual Citizenship of Lesbians and Gay Men in the United States*, 3 SEXUALITY RES. & SOC. POL'Y: J. OF NSRC 33-49 (2006), http://www.ucop.edu/lgbtia/mental%20health%20marriage%20denial.pdf (connecting denial of same-sex marriage rights and negative mental health outcomes).

[65] András Tilcsik, *Pride and Prejudice: Employment Discrimination Against Openly Gay Men in the United States*, 117 AM. J. SOC. 586, 586 (2011), http://www.jstor.org/stable/pdf/10.1086/661653.pdf.

[66] *Id.*

researchers found that "gay job applicants were approximately 40% less likely to be offered a job interview than their heterosexual counterparts."[67] Regional variations on this percentage, however, were heavily skewed; discriminatory tendencies were stronger in southern and midwestern states and weaker in western and northeastern states.[68]

The data generally corresponded to areas where more states offer anti-discrimination protections. No states in the South offer protections, and only Minnesota, Iowa, and Illinois offer legal protections for all LGBTQ people within the Midwest.[69] In contrast, four of five states bordering the Pacific Ocean offer full protections and all states in New England offer some type of protection.[70] The study analyzed nationwide trends rather than state legal protections and consequently focused on employment callback discrimination, which is harder for individuals to enforce than on-the-job discrimination.[71]

Transgender people face even more pervasive discrimination in employment and other areas, as shown by a nationwide survey of 6,450 transgender or gender nonconforming individuals from all 50 states.[72] Nine out of ten transgender individuals reported being harassed or discriminated against at work in some way; 47% experienced an adverse job action; and 26% were fired simply for being transgender.[73] Transgender people also faced similar discrimination in regard to housing. The study reported that 19% of respondents had been denied housing, 11% had been evicted, and 19% had been homeless at some point, all directly because they were transgender.[74] The rationale behind this discrimination is simple: many people — notably evangelical Christians — believe that transgender people are immoral and therefore do not deserve protected rights.[75]

These striking numbers show a population who struggles significantly with issues most people are unaware of: being discriminated

---

[67] *Id.* at 614.

[68] *Id.*

[69] *See* Non-Discrimination Laws: State by State Information – Map, AM. CIVIL LIBERTIES UNION, https://www.aclu.org/map/non-discrimination-laws-state-state-information-map (last visited Feb. 4, 2017).

[70] *See id.*

[71] Tilcsik, *supra* note 65, at 615-16.

[72] JAIME M. GRANT, LISA A. MOTTET, JUSTIN TANIS, JACK HARRISON, JODY L. HERMAN & MARA KEISLING, INJUSTICE AT EVERY TURN: A REPORT OF THE NAT'L TRANSGENDER DISCRIMINATION SURVEY 2 (Nat'l Ctr. for Transgender Equal. and Nat'l Gay and Lesbian Task Force eds., 2011), http://www.thetaskforce.org/static_html/downloads/reports/reports/ntds_full.pdf.

[73] *Id.* at 53.

[74] *Id.* at 106.

[75] Camille Beredjick, *Study: Most Evangelicals Think Transgender People Are Immoral*, PATHEOS (July 16, 2016), http://www.patheos.com/blogs/friendlyatheist/2016/07/16/study-most-evangelicals-think-transgender-people-are-immoral/.

against and the resulting adverse consequences. Because federal law and several states fail to protect LGBTQ people from these outcomes, alternative legal strategies must be examined.

C. BACKGROUND OF FEDERAL LAWS PROTECTING HEALTH DATA PRIVACY

Personal health data collection began in the 1920s and was traditionally kept on paper.[76] In the 1960s, universities began to create computer systems for healthcare providers, but it wasn't until the 1980s and 1990s that widespread use of electronic healthcare records took hold.[77] As computer technology advanced, so did the risks involved with storing sensitive data on computers.[78] Congress passed a series of laws beginning in 1996 that protect the privacy of personal health data; some of these laws are discussed herein.

1. HIPAA

The Health Information Portability and Accountability Act of 1996 (HIPAA) was landmark legislation that sought to address rapidly evolving technology in the field of health information storage and collection.[79] The purpose of this section is to explain important terms and definitions of HIPAA as well as describe in some detail the many complex requirements that HIPAA has imposed on healthcare providers, namely the promulgated regulations known as the "Privacy Rule," the "Security Rule," and the "Enforcement Rule." These three rules constitute the majority of provisions that apply directly to healthcare providers, and are the focus of HIPAA compliance.

HIPAA defines "individually identifiable health information" as any information created or received by any healthcare provider that relates to a health condition and identifies an individual by name or through inference.[80] Some of this information is called "protected health information" (hereafter, PHI).[81]

---

[76] Ashley Brooks, *Health Information Management History: Past, Present & Future*, RASMUSSEN COLL. SCH. OF HEALTH SCIS. BLOG (Mar. 23, 2015), http://www.rasmussen.edu/degrees/health-sciences/blog/health-information-management-history/.

[77] *Id.*

[78] *Id.*

[79] *See* Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,182, 53,182 (Aug. 14, 2002) (to be codified at 45 C.F.R. § 160 and 45 C.F.R. § 164).

[80] 42 U.S.C. § 1320d(6) (2015).

[81] 45 C.F.R. § 160.103 (2016) (defining PHI as individually identifiable health information that is stored or transmitted in electronic media or other media except that information in employment records and for people deceased for over fifty years).

HIPAA's Privacy Rule mandates the maintenance of "appropriate administrative, technical, and physical safeguards" to preserve PHI.[82] Only in very limited circumstances may PHI be disclosed.[83] The regulations simultaneously grant access to individuals of their own health information[84] while restricting disclosure for all other purposes except coordinating the individual's treatment or payment for services and other minor exceptions.[85]

The Security Rule focuses on the transmission of electronically stored health information in order to "[e]nsure the confidentiality, integrity, and availability of all electronic protected health information . . . ."[86] This rule provides physical safeguards such as mandatory disposal and re-use of media requirements,[87] as well as process safeguards such as mandatory risk analysis.[88] Additionally, the Security Rule requires technical safeguards involving unique user identification on computer systems and provides conduct guidelines during emergencies.[89]

The Enforcement Rule allows the HHS Office of Civil Rights ("OCR") to levy civil fines on covered entities that violate the Privacy and Security rules.[90] The rule came into effect just under ten years after Congress passed HIPAA, on March 16, 2006.[91] Enforcement provisions for breaching duties owed under HIPAA include civil fines and criminal prosecution. Until February 18, 2009, the maximum fine was $100 per violation up to a maximum of $25,000 per calendar year.[92] However, between 2006 and 2009, when the Privacy Rule and the Enforcement Rule came into effect, zero civil fines were imposed and only two cases were criminally prosecuted.[93]

Since 2009, when the Health Information Technology for Economic and Clinical Health Act (HITECH) passed, the minimum fine is $100 per violation in no-fault cases, and in cases of willful neglect is $50,000 per violation, up to a maximum of $1,500,000 per violator per calendar

---

[82] 42 U.S.C. § 1320d-2(d)(2) (2015).

[83] *See* 45 C.F.R. § 164.502(b)–(j) (2016) (explaining a limited number of circumstances in which PHI may be disclosed, including to parents of minors, its own business associates, and representatives of a deceased person's estate).

[84] *See id.* at § 164.524(a)(1) (2016).

[85] *See id.* at § 164.502(a) (2016).

[86] *Id.* at § 164.306(a)(1) (2016).

[87] *See id.* at § 164.310 (2016).

[88] S*ee id.* at § 164.308 (2016).

[89] *See id.* at § 164.312 (2016).

[90] *Id.* at § 160.402(a) (2016).

[91] HIPAA Administrative Simplification: Enforcement, 71 Fed. Reg. 8389, 8390 (Feb. 16, 2006).

[92] 45 C.F.R. § 160.404(b)(1) (2016).

[93] Rob Stein, *Medical Privacy Law Nets No Fines*, WASH. POST (June 5, 2006), http://www.washingtonpost.com/wp-dyn/content/article/2006/06/04/AR2006060400672.html.

year.[94] At its peak in 2014, OCR reviewed 239 cases and 90% of these resulted in civil penalties.[95] Civil penalties generally only affect the corporation involved with the noncompliance while criminal penalties are more narrowly tailored to preventing individual malfeasance.

HHS may also refer cases to the Department of Justice for criminal investigations — an offender who wrongfully discloses individually identifiable health information may serve a sentence of up to one year in prison.[96] Offenses committed under false pretenses carry prison sentences up to five years, and if the information is used for commercial or personal gain or is otherwise malicious, a ten-year sentence can be levied.[97]

Criminal hackers will continue to seek protected personal information as long as enforcement remains lax because the benefits outweigh the risks. Although enforcement may currently be subpar, Congress has supplemented the rules with additional legislation.

2. HITECH

In addition to raising the maximum civil and criminal penalties for violations of HIPAA privacy protections, the Health Information Technology for Economic and Clinical Health Act ("HITECH") added new protections for electronic health records and mandated data breach reporting.[98] The mandated data breach reporting was a major step forward in enforcing the HIPAA rules.

To protect patients, HITECH implemented detailed notice requirements. For example, notice must be given to all affected individuals in writing. Substitute forms of notice must be given if the contact information is out of date.[99] Entities that must provide notice include: health care providers, such as doctors and pharmacies; health plans, such as insurance companies and HMOs; and healthcare clearinghouses, such as data analysis companies.[100] If more than 500 patients are affected by a single

---

[94] 45 C.F.R. § 160.404(b)(2) (2016).

[95] U.S. Dep't of Health & Human Servs., *Enforcement Results by Year — Compliance Reviews*, HHS.GOV: HEALTH INFORMATION PRIVACY, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/results-by-year-compliance-reviews/index.html (last visited Feb. 7, 2017).

[96] 42 U.S.C. § 1320d-6(b) (2015); *see also* 45 C.F.R. § 160.418 (2016).

[97] 42 U.S.C. § 1320d-6(b) (2015).

[98] Morgan, Lewis & Bockius LLP, *HIPAA/HITECH Enforcement Action Alert*, NAT'L LAW REVIEW (Mar. 22, 2012), http://www.natlawreview.com/article/hipaahitech-enforcement-action-alert; *see generally* Medicare and Medicaid Programs; Electronic Health Record Incentive Program, 75 Fed. Reg. 44,314 (July 28, 2010).

[99] 45 C.F.R. § 164.404(d) (2016).

[100] *Id.* at § 160.103 (2016) (defining "covered entity"); *see also* U.S. Dep't of Health & Human Servs., *Covered Entities and Business Associates*, HHS.GOV: HEALTH INFORMATION PRI-

breach, the covered entity must notify prominent local media outlets as well.[101] In all cases, covered entities must contact the Secretary of HHS, who will then forward the information to the HHS Office of Civil Rights, which is in charge of enforcement.[102]

HITECH also set aside $25.9 billion for eligible hospitals and medical professionals to encourage and facilitate the adoption of electronic health records.[103] As a result, 97% of hospitals in the United States had certified electronic health records technology by 2014.[104]

Although HITECH provided fewer substantive protections than HIPAA, its provisions are still worth noting due to the upward progression federal health data protections. While this trend is a positive omen that protections are moving in the right direction, it remains insufficient to fully protect all patients.

3. Affordable Care Act

The Patient Protection and Affordable Care Act ("ACA"), President Obama's largest piece of landmark legislation, is best known for creating health insurance marketplaces in most states and providing health insurance to millions of previously uninsured people. The most relevant parts of the ACA in regard to privacy concerns of LGBTQ people are its provisions for mandated compliance with electronic transaction standards and collection of personal health data to better treat at-risk populations.

The ACA requires health plans, defined as all health providers providing healthcare to 50 or more people, including Medicare and Medicaid,[105] to obtain certification that it is in compliance with electronic transaction standards covering claims, electronic fund transfers, and healthcare payments.[106] A nationwide nonprofit, the Council for Affordable Quality Healthcare ("CAQH"), developed a set of operating rules called CORE that is designated by the HHS Secretary as the standard for

---

VACY, http://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html (last visited Feb. 7, 2017).

[101] 45 C.F.R. § 164.406(a) (2016).

[102] *Id.* at § 164.408 (2016).

[103] Michael L. Tudor, *Protecting Privacy of Medical Records of Employees and Job Applicants in the Digital Era Under the Americans With Disabilities Act*, 40 N. KY. L. REV. 635, 635 (2013), http://mynkuhelp.nku.edu/content/dam/chaselaw/docs/academics/lawreview/v40/nklr_v40n3_pp635-663.pdf.

[104] DUSTIN CHARLES, MEGHAN GABRIEL & TALISHA SEARCY, ADOPTION OF ELECTRONIC HEALTH RECORD SYSTEMS AMONG U.S. NON-FEDERAL ACUTE CARE HOSPITALS: 2008-2014 1 (Office of the National Coordinator for Health Information Technology, ed. 2015), https://www.healthit.gov/sites/default/files/data-brief/2014HospitalAdoptionDataBrief.pdf.

[105] *See* 42 U.S.C. § 1320d(5) (2015).

[106] *Id.* at § 1320d-2(h) (2015).

certification under the ACA.[107] Originally, all health plans were required to register all certification by December 31, 2015, but the final regulation was not implemented by that date.[108] CAQH is currently rewriting the rule to enforce certification in the future.[109]

The ACA also affected public policy regarding data collection. The law itself only provides measures for collecting health disparity data on race, ethnicity, sex, primary language, and disability status.[110] Since Congress passed the law, however, HHS developed policies to collect data on sexual orientation and gender identity, categories determined by the HHS Secretary to be appropriate for collection.[111] The wealth of personal information contained in this data exponentially increases the risk for data hacking specifically aimed at groups who are traditional targets of hatred.

The current scheme of health data protection laws, the lack of anti-discrimination laws at the federal and state levels, and the LGBTQ population's vulnerability to discrimination leave a huge hole in the effort to prevent negative outcomes. It is beneficial to collect this data, but protecting LGBTQ people's personal information from disclosure is of the utmost importance. The fundamental thing is to create specific protections for LGBTQ people to prevent them from needing to be hidden, ashamed, or secretive.

D. Rationale for Collecting Health Data from LGBTQ Individuals

The medical establishment consistently seeks to improve its patient treatment modalities, and after discovering disparities in the care of LGBTQ people compared to other populations, it began studying health trends that affect the LGBTQ population.[112] Researchers discovered powerful data indicating that LGBTQ healthcare disparities exist not because of any genetic or inherent difference, but because of bias, stigma, and discrimination.[113] Health problems especially faced by LGBTQ peo-

---

[107] *CORE Certification*, Council for Affordable Quality Healthcare, http://www.caqh.org/core/core-certification (last visited Feb. 6, 2017).

[108] 42 U.S.C. § 1320d-2(h)(1)(B) (2015).

[109] Council for Affordable Quality Healthcare, *supra* note 107.

[110] 42 U.S.C. § 1396w-5(a) (2015).

[111] *Id.* at § 300kk(a)(1)(D) (2013); *Improving Data Collection for the LGBT Community*, Office of Minority Health, http://minorityhealth.hhs.gov/omh/browse.aspx?lvl=3&lvlid=57 (last updated Sept. 9, 2013).

[112] Joe Alper, Monica N. Feit & Jon Q. Sanders, Collecting Sexual Orientation and Gender Identity Data in Electronic Health Records: Workshop Summary 5-6 (2013), https://www.ncbi.nlm.nih.gov/books/NBK132859/pdf/Bookshelf_NBK132859.pdf.

[113] *Id.* at 5.

ple include: psychiatric disorders, substance abuse, high rates of suicide, HIV/AIDS, other sexually transmitted diseases, and lack of access to treatment.[114] The researchers found that these disparities can only be addressed if providers collect data about this population in order to identify statistical trends.[115]

Implementing collection of "sexual orientation and gender identity" ("SOGI") data at a wider variety of sites, such as hospitals and universities that conduct health research, would lead to better treatment of LGBTQ people consistent with the goals set out by federal policy, which as of 2010 includes data collection from these populations in order to "document, understand, and address the environmental factors that contribute to health disparities" among the LGBTQ population.[116] However, the full implementation of these policies could create a paradox in which data collected under color of law would indirectly result in discrimination.

HHS releases public health objectives every ten years called Healthy People. Healthy People 2020, which was released in December 2010, included "Lesbian, Gay, Bisexual, and Transgender Health" as a ten-year health objective for the first time.[117] A supplement to Healthy People 2010, released in 2000, focused only on the ways other objectives including mental health, substance abuse, and HIV/AIDS would improve LGBTQ health.[118] An academic journal also focused on the imminent need for SOGI data collection to better monitor the aforementioned areas of LGBTQ health.[119]

Health providers have already begun to implement these data collection programs and have been seeing results. The federal government during the Obama administration developed a plan to integrate SOGI data into its surveys of national health.[120] Many prominent health clinics and providers, including The Mayo Clinic, Kaiser Permanente, Fenway Health, and Vanderbilt University, already collect SOGI data.[121]

---

[114] *See Lesbian, Gay, Bisexual, and Transgender Health*, HEALTHYPEOPLE.GOV (last visited Feb. 7, 2017), http://www.healthypeople.gov/2020/topics-objectives/topic/lesbian-gay-bisexual-and-transgender-health.

[115] ALPER, ET AL., *supra* note 112, at 6.

[116] HEALTHYPEOPLE.GOV, *supra* note 114.

[117] *2020 Topics and Objectives – Objectives A-Z*, HEALTHYPEOPLE.GOV, http://www.healthypeople.gov/2020/topics-objectives (last visited Feb. 7, 2017).

[118] Randall L. Sell & Jeffrey Blake Becker, *Sexual Orientation Data Collection and Progress Toward Healthy People 2010*, 91 AM. J. PUB. HEALTH 876, 877 (2001), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1446460/pdf/11392926.pdf.

[119] *Id.* at 876 (discussing the need for data collection because of federal policy seeking to monitor lesbian, gay, and bisexual sexual health, HIV/AIDS trends, violence against LGB people, mental health, and substance abuse).

[120] ALPER, ET AL., *supra* note 112, at 15-17.

[121] ALPER, ET AL., *supra* note 112, at 29-35.

One of the nation's top LGBTQ health clinics, the Fenway Institute in Boston, conducted a study that recommends the standard for asking questions about SOGI in clinical settings.[122] A 2005 study showed that 61% of gay and bisexual men did not voluntarily disclose their sexual orientation to their doctors, which leads to lack of cultural competency in their care.[123] This fact is highly damaging to population-specific healthcare and can only be remedied by taking away the negative societal pressures LGBTQ people face to hide their identities.

Current federal policy is moving in the right direction, but more effort must be made to treat these populations. However, even if all these goals were accomplished, the danger of health data breaches leaking personally identifiable SOGI data presents a dire problem that must be remedied, as presented below.

II. ARGUMENT

A. HEALTH DATA BREACHES WILL INEVITABLY CAUSE IMPERMISSIBLE DISCRIMINATION AGAINST LGBTQ PEOPLE

The federal government continually refuses to pass meaningful LGBTQ anti-discrimination legislation and states vary drastically in their protections or burdens. LGBTQ people experience discrimination in unacceptable amounts and with deplorable consequences, such as severe bullying leading to suicide.[124] With the advent of all-electronic health data storage and an unprecedented level of computer hacking, LGBTQ people are at a higher risk than ever of losing their data to unknown, malicious parties.

All of these factors together create an impasse when combined with new policies to collect data that include an individual's sexual orientation and gender identity. Connecting this new type of data collection with the risk of the data being breached will lead to further discrimination. There are a number of possible solutions to this problem, but the problem must first be recognized and presented for consideration.

---

[122] THE FENWAY INSTITUTE & THE CENTER FOR AMERICAN PROGRESS, ASKING PATIENTS QUESTIONS ABOUT SEXUAL ORIENTATION AND GENDER IDENTITY IN CLINICAL SETTINGS: A STUDY IN FOUR HEALTH CENTERS 2 (2013), http://www.thefenwayinstitute.org/wp-content/uploads/COM228_SOGI_CHARN_WhitePaper.pdf.

[123] *Id.* at 5.

[124] Ed Pilkington, *Tyler Clementi, Student Outed as Gay on Internet, Jumps to His Death*, THE GUARDIAN (Sept. 30, 2010, 4:08 PM), https://www.theguardian.com/world/2010/sep/30/tyler-clementi-gay-student-suicide.

1. Health Data Breaches

Hackers and data miners pursue sensitive and valuable information. In a culture that either actively or passively permits discrimination against LGBTQ people in 33 out of 50 states, people who wished to exclude those groups could potentially use data that states a person's sexual orientation or gender identity.

The sheer number of data breaches paints a grave picture. Data breaches have become so commonplace that only major breaches even get media attention. A corporate data breach costs the company on average $3.79 million.[125] A full 65% of American corporations surveyed experienced some type of data breach in 2014.[126]

The incentive for hackers to obtain medical information is high: remember that a Medicare number with other personally identifiable information can sell on the black market for almost $500,[127] as opposed to a stolen credit card, which nets merely $12.[128] Even in less sophisticated criminal groups, medical information can sell for at least ten times as much as a credit card number.[129] Medical information is also valuable because of its other potential uses: identity theft, false insurance claims, and blackmail.[130]

Health data breaches are also the most costly to affected entities. The per capita cost of a health data breach is $363 per person — over double that of a retail data breach.[131] Additionally, health care companies experienced a 72% increase in cyber-attacks from 2013 to 2014.[132]

Health data breaches result in numerous consequences for affected individuals. In addition to losing trust in healthcare providers, affected individuals have reported misdiagnoses of illnesses, delays in receiving medical treatment, mistreatment of illness, and wrong pharmaceuticals being prescribed.[133] A great number, 65%, of affected individuals also suffered financial consequences due to lost time and productivity, lower

[125] PONEMON INSTITUTE, 2015 COST OF DATA BREACH STUDY: GLOBAL ANALYSIS 1 (2015), https://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.pdf.

[126] CYBER EDGE GROUP, 2015 CYBERTHREAT DEFENSE REPORT: NORTH AMERICA & EUROPE 8 (2015), http://www.novell.com/docrep/2015/03/CyberEdge_2015_CDR_Report.pdf.

[127] Aarti Shahani, *The Black Market for Stolen Health Care Data*, NPR: ALL TECH CONSIDERED (Feb. 13, 2015), http://www.npr.org/sections/alltechconsidered/2015/02/13/385901377/the-black-market-for-stolen-health-care-data.

[128] Skowronski, *supra* note 4.

[129] Abelson & Goldstein, *supra* note 5.

[130] *Id.*

[131] PONEMON INSTITUTE: COST OF DATA BREACH STUDY, *supra* note 125, at 9.

[132] Shahani, *supra* note 127.

[133] PONEMON INSTITUTE, 2013 SURVEY ON MEDICAL IDENTITY THEFT 8 (2013), http://www.ponemon.org/local/upload/file/2013%20Medical%20Identity%20Theft%20Report%20FINAL%2011.pdf.

credit score, legal fees, fraudulent bills, and employment-related difficulties such as discipline or lost wages due to time taken off from work in order to address these issues.[134] For LGBTQ people, who already experience workplace discrimination and healthcare disparities, the effect of a breach could be even more severe.

The consequences of health identity theft can also be aggravated by the length of time before the patient discovers the breach. Only 9% of patients discover theft because of legally mandated breach notifications.[135] More common methods of theft discovery include errors in medical invoices, collection letters for services not rendered, mistakes in health records, and adverse entries on credit reports.[136] These methods often take substantial amounts of time before the patient discovers the theft, which allows data thieves more time to illegally use the information.

2. Data Breaches and Discrimination

In the past, most medical identity theft occurred because of people known to the victim — family members, friends, and others with access to a person's personal information. Today, people known to the patient account for a decreasing amount of medical identity theft — down from 58% in 2013 to 47% in 2014.[137] Inversely, data breaches and phishing scams have increased in share — up from 15% in 2013 to 24% in 2014.[138] Since 2009, more than 120 million people have had their personal health data compromised in some way — over one third of the United States population.[139]

To prevent further harm from occurring, our society must attack this problem from all fronts, including finding and punishing criminals who perpetrate these crimes, strengthening our laws and regulatory schemes, and providing further incentives and penalties to advance compliance.

The hackers responsible for the interception of health data are widely believed to be primarily Chinese and Russian nationals[140] — citi-

---

[134] *Id.* at 9.

[135] PONEMON INSTITUTE, FIFTH ANNUAL SURVEY ON MEDICAL IDENTITY THEFT 11 (2015), http://medidfraud.org/wp-content/uploads/2015/02/2014_Medical_ID_Theft_Study1.pdf.

[136] *Id.*

[137] *Id.* at 13.

[138] *Id.*

[139] Andrea Peterson, *2015 Is Already the Year of the Health-Care Hack — and It's Only Going to Get Worse*, WASH. POST: THE SWITCH (Mar. 20, 2015), http://www.washingtonpost.com/news/the-switch/wp/2015/03/20/2015-is-already-the-year-of-the-health-care-hack-and-its-only-going-to-get-worse/.

[140] Michael Riley & John Walcott, *China's Hack of U.S. Data Tied to Health-Care Record Thefts*, BLOOMBERG BUSINESS (June 4, 2015), http://www.bloomberg.com/news/articles/2015-06-05/

zens of countries without United States extradition treaties[141] — who are believed to be selling health data on the black market for profit. However, hackers also exist in the United States, and some of them may be homophobic or transphobic. There is no shortage of evidence of animus against LGBTQ people in the United States.[142] Considering the panic and ensuing witch-hunt surrounding transgender people using bathrooms in North Carolina after HB 2 passed in early 2016,[143] a situation is not unthinkable in which homophobic or transphobic individuals begin a technology-driven pursuit to out LGBTQ individuals by hacking into their health data. A similar situation already occurred in 2014 when hackers published the names of 37 million Ashley Madison users in order to out them by putting the proverbial scarlet letter on their chests. In the case of attacking LGBTQ people, however, the consequences could be much graver.

The time for legislative reform to increase protection and compliance is now, given HHS's new data collection policies to improve the healthcare of LGBTQ individuals. These policies are excellent for proponents of specialized healthcare and the LGBTQ population at large, but they may add significantly to LGBTQ people's potential harm when combined with increasing numbers of data breaches.

A published list of names with other personally identifiable information of LGBTQ people could be catastrophic. Employers in states that do not provide anti-discrimination protections could maintain do-not-hire lists, or fire all their LGBTQ employees without notice. State agencies and private landlords could automatically deny people from renting or buying a home. This dystopian nightmare is not that far of a stretch.

---

u-s-government-data-breach-tied-to-theft-of-health-care-records; Jessica Davis, *Medical Data of U.S. Olympic Athletes Leaked by Russian Hackers*, HEALTHCARE IT NEWS (Sept. 14, 2016, 11:25 AM), http://www.healthcareitnews.com/news/medical-data-us-olympic-athletes-leaked-russian-hackers.

[141] *See* 18 U.S.C. § 3181 note (2015).

[142] *See generally, e.g.*, BRAD SEARS, NAN D. HUNTER & CHRISTY MALLORY, THE WILLIAMS INSTITUTE, DOCUMENTING DISCRIMINATION BASED ON SEXUAL ORIENTATION AND GENDER IDENTITY IN STATE EMPLOYMENT (2009); Nicholas Pedriana, *Intimate Equality: The Lesbian, Gay, Bisexual, and Transgender Movement's Legal Framing of Sodomy Laws in the* Lawrence v. Texas *Case, in* QUEER MOBILIZATIONS: LGBT ACTIVISTS CONFRONT THE LAW 52-75 (Scott Barclay et al. eds., 2009).

[143] *See, e.g.*, Ellie DeLano, *One Woman Had a Strange, Eye-Opening Encounter in a Target Bathroom*, UPWORTHY (May 11, 2016), http://www.upworthy.com/one-woman-had-a-strange-eye-opening-encounter-in-a-target-bathroom (describing a woman's experience shopping at a Target store, which publicly proclaimed at the time a trans-inclusive bathroom policy, affirming its guests' ability to use the bathroom of their choice); Sarah K. Burris, *Small Bomb Blows Up Target Bathroom While Company Faces Right-Wing Wrath for Transgender Policy*, RAW STORY (June 9, 2016), http://www.rawstory.com/2016/06/small-bomb-blows-up-target-bathroom-while-company-faces-right-wing-wrath-for-transgender-policy/ (describing a bomb set presumably by a right-wing transphobic activist in an Evanston, Illinois Target store in response to the same policy).

Until the federal and state legislatures pass appropriate legislation or the Supreme Court decides that LGBTQ people are protected classes under Equal Protection, deserving of heightened constitutional scrutiny, the state and federal executive branches must continue to mitigate negative impacts on vulnerable populations by focusing on the roots of problems in its executive branch policies.

Health data privacy does not face the same roadblocks in the legislature as rights for LGBTQ people. Health data privacy is already an important priority for the federal government, considering the three landmark pieces of legislation made into law in the last twenty years — HIPAA, HITECH, and the ACA. Currently, LGBTQ people who choose to seek remedies for health data breaches face a dire decision. If an LGBTQ individual chooses to file a lawsuit alleging a violation of their privacy right, they run the risk of making their sexual orientation or gender identity public through court records. If they decide not to file in order to protect their privacy, they suffer in silence. The current options are insufficient and do not protect LGBTQ people. However, there are a number of possible remedies that the government and private companies can implement in order to lessen these risks.

B. Suggested Remedies to Prevent Discrimination Against LGBTQ People

In the absence of meaningful legislation that protects LGBTQ people, there are other methods to protect them. In the realm of computer hacking of health data, a comprehensive solution requires resources, diligence, and effort. However, the benefits of compliance include not only stronger protections for LGBTQ people, but also lower risks of data breaches and huge long-term company cost savings. It is a win-win situation for the LGBTQ population, companies, and the general public.

1. Compliance

a. Security Infrastructure

In the movies, computer systems frequently become sentient and malicious;[144] in real life, only humans are capable of breaching computer information. Because people cause data breaches, people are the only way to stop the release of data. The standards presented in HIPAA and related legislation would be sufficient to protect patient health data if it

[144] *See* 2001: A Space Odyssey (Metro-Goldwyn-Mayer 1968); The Terminator (Orion Pictures 1984); WarGames (MGM/UA Entm't Co. 1983).

were followed to the letter. However, high costs, a shortage in competent information technology employees, and lack of incentive make compliance difficult.[145]

High cost is a top reason for security noncompliance. Regulatory compliance is undoubtedly a business decision — the benefits must outweigh the costs. The average cost for achieving regulatory compliance is $3.5 million per company.[146] This is close to the reported cost for an average data breach, $3.79 million per incident.[147] However, upon closer inspection, when additional costs related to the breach are included like "business disruption, reduced productivity, fees, penalties and other legal and non-legal settlement costs," the overall price raises to $9.4 million per incident.[148] This stark difference would seem to suggest that there is no reason for companies *not* to comply, but the number of data breaches still occurring paints a different picture.

Lack of enforcement also plays into companies' decisions not to comply with the law. Even repeat blatant offenders of HIPAA privacy laws are often not scrutinized and penalized — the HHS Office of Civil Rights warned CVS Pharmacy over two hundred times between 2011 and 2014 to stop violating laws, but throughout HIPAA's lifetime, HHS fined CVS only once for $2.25 million.[149]

Even when companies achieve full regulatory compliance, patient data may still be at risk for breach. Data encryption is the industry standard in the technology sector, and protects everything from copyrighted information to credit card processing to website user data.[150] However, HIPAA does not mandate data encryption, so companies that are in full regulatory compliance may still have major security holes.

---

[145] Stephanie Tayengco, *Why Are Healthcare Data Breaches So Common?*, BECKER'S HEALTH IT & CIO REVIEW (Sept. 17, 2015), http://www.beckershospitalreview.com/healthcare-information-technology/why-are-healthcare-data-breaches-so-common.html.

[146] Ellen Messmer, *Cost of Regulatory Security Compliance? On Average, $3.5M*, NETWORK WORLD (Jan. 31, 2011, 12:00 AM), http://www.networkworld.com/article/2199260/compliance/cost-of-regulatory-security-compliance—on-average—-3-5m.html.

[147] PONEMON INSTITUTE: COST OF DATA BREACH STUDY, *supra* note 125, at 1.

[148] Messmer, *supra* note 146.

[149] Charles Ornstein & Annie Waldman, *Repeat Violators of Health Privacy Laws Often Go Unpunished*, SHOTS: HEALTH NEWS FROM NPR (Dec. 29, 2015, 4:00 AM), http://www.npr.org/sections/health-shots/2015/12/29/460828382/few-consequences-for-health-privacy-laws-repeat-offenders.

[150] *DRM*, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/issues/drm (last visited Nov. 1, 2016); Nicole Perlroth & David E. Sanger, *Obama Won't Seek Access to Encrypted User Data*, N.Y. TIMES, Oct. 10, 2015, http://www.nytimes.com/2015/10/11/us/politics/obama-wont-seek-access-to-encrypted-user-data.html?_r=0; *Secure Data Encryption*, SQUARE, INC., https://squareup.com/help/us/en/article/3797-secure-data-encryption (last visited Nov. 1, 2016).

"The key is risk management," said Kevin Cureton, a data security expert.[151] Regular compliance audits are a necessity, but 28% of companies do not conduct them at all, and of the ones that do, only 11% of them conduct them five or more times per year.[152] There are many resources available to companies seeking to be compliant, such as the National Institute of Standards and Technology's Cybersecurity Framework ("NIST").[153] While the NIST Cybersecurity Framework does not provide a list of actionable tasks, it provides excellent guidance to companies seeking to be in compliance with regulations that are applicable to them.[154]

Healthcare companies have the option of using their own internal Information Technology ("IT") departments or hiring outside consultants to achieve data security and regulatory compliance. Many companies, to save costs and keep knowledge internal, choose to keep security-related tasks in-house rather than hiring outside companies, but often do not have the resources to train their employees with rapidly changing standards.[155]

Cloud services — data systems and networks that exist entirely on the internet — are relatively new, but the top providers such as Amazon Web Services ("AWS"), Rackspace, Microsoft Azure, and Google Cloud Computing provide greatly enhanced protection for data.[156] Storing data in the cloud entrusts cloud providers with many traditional security problems, such as unauthorized access to server rooms, audit controls, and user access controls. To combat these problems, Amazon Web Services advertises and explains how to use their tools to comply with HIPAA requirements.[157] Amazon Web Services increases their clients' data security because "the odds of someone breaching AWS and getting access to your [data] [are] likely zero."[158]

The demand for competent IT departments outstrips the supply, which is another cause of data breaches. This affects both large compa-

---

[151] Interview with Kevin Cureton, Senior Systems Engineer, Nimble Collective, Inc., in S.F., Cal. (Jan. 21, 2016).

[152] Messmer, *supra* note 146.

[153] *See* NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (2014), http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

[154] Cureton Interview, *supra* note 151.

[155] *See* Mary K. Pratt, *Where Does Security Fit in Bi-Modal IT Departments?*, CSO ONLINE (Sept. 16, 2015, 5:05 AM), http://www.csoonline.com/article/2984412/infosec-staffing/where-does-security-fit-in-bi-modal-it-departments.html.

[156] Cureton Interview, *supra* note 151.

[157] AMAZON WEB SERVICES, ARCHITECTING FOR HIPAA SECURITY AND COMPLIANCE ON AMAZON WEB SERVICES (2017), https://d0.awsstatic.com/whitepapers/compliance/AWS_HIPAA_Compliance_Whitepaper.pdf.

[158] Cureton Interview, *supra* note 151.

nies, who cannot always hire the best of the best, and small companies, who may not be able to have adequate, if any, IT staff.[159] Better training in regulatory matters and holistic data security could go far for companies who need to secure health data.[160]

Increases in security infrastructures will accomplish much of what is needed to comply with the HIPAA Security and Privacy rules and protect sensitive health data, but more can still be done.

b. Incentives for Compliance

HIPAA has been in effect for nearly twenty years, and its Enforcement Rule for ten years, but compliance is still fairly uncommon. Encouragement of compliance can come in two forms: incentives and penalties.

Congress passed some significant financial incentives as part of various laws to encourage compliance with HIPAA. As previously mentioned, HITECH included a $25.9 billion appropriation of funds to encourage healthcare providers to adopt electronic health records. The track record of healthcare providers in actually protecting sensitive patient health data is poor and the government's stake in protecting its constituents is too high to quarrel over budgetary line items.

Congress's effort to encourage use of electronic health records was successful, but they have inadequately addressed the protection of those records. Congress needs to take the next logical step: providing funds and resources to enforce the laws and protecting their constituents. Currently, smaller health providers often do not have the resources to comply fully with regulations, and larger companies are attractive targets for hackers because of the breadth of information available in one place. Therefore, the congressional budget should include new funds for healthcare companies and providers to comply with HIPAA privacy and security safeguards, supplemented by the newly raised penalties as described below.

Congress should also authorize additional penalties on noncompliant companies. Raising the cap of $1.5 million per incident may seem draconian, but it may not be enough to strong-arm large companies into full compliance. Anthem Blue Cross, which suffered a breach in January 2015 that affected as many as 80 million people,[161] has an annual profit

[159] *Id.*

[160] *Id.*

[161] Michael Hiltzik, *Anthem Is Warning Consumers About Its Huge Data Breach. Here's a Translation.*, L.A. TIMES (Mar. 6, 2015, 10:34 AM), http://www.latimes.com/business/hiltzik/la-fi-mh-anthem-is-warning-consumers-20150306-column.html.

of over $2.5 billion.[162] Even considering the numerous additional costs — credit monitoring and other services that a breached company must provide to affected consumers — a $1.5 million penalty will not encourage Anthem to increase their data security. Thus, the cap on penalties under HIPAA should be drastically increased on a sliding scale. This action would serve as a warning to noncompliant providers, and effect the same result as punitive damages would if a private right in tort existed.

2. Enforcement

a. New Right in Tort Under HIPAA

While HHS has the ability to levy civil fines and prosecute criminals under HIPAA, there is still a giant hole in remedies available to victims of data breaches. Specifically, Congress did not create a private right in tort under HIPAA.[163] Because a suit for HIPAA-noncompliance resulting in damages would address a failure to protect data instead of LGBTQ discrimination, it does not run the same risks of outing an LGBTQ individual as a suit regarding direct discrimination.

Plaintiffs have brought a few successful cases against healthce companies for violations of privacy. In 2006, plaintiff Heather Acosta sued her doctor for improperly accessing her medical records.[164] She sued in North Carolina state court on a theory of negligent infliction of emotional distress and invasion of privacy and the court dismissed her case for failure to state a claim.[165] On appeal, the court reversed Acosta's dismissal.[166] The North Carolina appellate court recognized that HIPAA set a duty of care that was breached by the doctor even though HIPAA did not afford a cause of action itself.[167] This case is one of the few examples of any plaintiff successfully recovering damages for an invasion of privacy.

One state, Connecticut, decided that HIPAA does not preempt state claims for damages.[168] However, there is no sign that this decision has

[162] ANTHEM, 2014 ANNUAL REPORT: REDEFINING REINVENTING REASSURING 12 (2014), http://media.corporate-ir.net/media_files/IROL/13/130104/2014AR/export7/pdfs/Anthem_2014AR.pdf.

[163] Edward Vishnevetsky, *Can A HIPAA Violation Give Rise to a Private Cause of Action?*, DALLAS/FORT WORTH HEALTHCARE DAILY (May 27, 2014), http://healthcare.dmagazine.com/2014/05/27/can-a-hipaa-violation-give-rise-to-a-private-cause-of-action/.

[164] Acosta v. Byrum, 638 S.E.2d 246, 249 (N.C. Ct. App. 2006).

[165] *Id.* at 248-49.

[166] *Id.* at 254.

[167] *Id.* at 253.

[168] *See* Byrne v. Avery Ctr. for Obstetrics & Gynecology, 102 A.3d 32, 36 (Conn. 2014).

affected other states' jurisprudence, so its usefulness as precedent is questionable.

Congress's creation of a federal right in tort under HIPAA would provide the necessary motivation for companies to effectively protect their patients' health data. Because these HIPAA tort claims would likely be numerous and similar to one another, Congress should assign the task of adjudicating these matters to administrative courts, which currently handle federal matters such as social security disability applications and Medicare appeals. The specter of countless tort claims in the aftermath of a data breach would not only protect the interests of consumers effectively, but would be enough of an incentive to ensure full protection in the future by that company and all others.

b. Increased Budget for HHS Office of Civil Rights

The HHS Office of Civil Rights (OCR) is responsible for all HIPAA-related investigations. This includes all levying of civil penalties, audits, policy writing, and business administration.[169] The OCR does this on a total budgetary allocation of $42,705,000, which increased less than $4 million from the previous year.[170] This number, while seemingly significant, is actually insufficient considering the ever-increasing number of data breaches to enforce. Enforcement of the current laws is the best way to encourage healthcare companies to protect their patients' PHI.

As the agency responsible for protecting individually identifiable health information, it is imperative that this office be funded to the greatest reasonable extent. Much of this increased budget may be able to come from the increased revenue gained by additional enforcement. Their ability to investigate and audit healthcare companies under the HIPAA Enforcement Rule is the only thing that gives HIPAA any clout. This is, of course, dependent on Congress increasing a budgetary allotment, but it is not a major expense in the grand scale of a congressional budget.

The HHS OCR enforces HIPAA violations and receives settlements. In 2014, the OCR collected a total of $7,940,220 from six healthcare companies with major HIPAA violations and then set up compliance plans with them.[171] This type of collection will increase HHS's budget as

[169] JOCELYN SAMUELS, OFFICE OF CIVIL RIGHTS FISCAL YEAR 2016 CONGRESSIONAL JUSTIFICATION 20 (Office of Civil Rights ed., 2015), http://www.hhs.gov/sites/default/files/budget/office-of-civil-rights-budget-justification-2016.pdf.

[170] *Id.* at 6.

[171] *Id.* at 22-23.

well, but the scale of the operations must increase further to achieve full enforcement.

III. CONCLUSION

The Hzone and Ashley Madison breaches showed how monetary gain was not always the objective for data hackers and the lengths some were willing to go to expose people they view as hypocritical or morally wrong. Unfortunately, many people in the United States still see gay and bisexual people, lesbians, and transgender people as moral failures, and they are therefore at risk of having their identities exposed by hackers.

Data breaches are of major concern to businesses in all sectors, but the stakes are highest in the healthcare sector. Electronic health records contain highly personal and sensitive information, and the publication of this information can be catastrophic to individuals — not to mention bad for business.

In theory, the legal protections offered to victims of data breaches are sufficient to protect their privacy rights, but in practice the protections fall short. The enforcement capabilities of the HHS Office of Civil Rights are limited by budgetary restrictions, Department of Justice officials are overworked, and affected individuals have no ability to protect their own interests past receiving free credit monitoring software.

The inherently sensitive nature of health data increases the importance of its protection. The potential of medical identity theft is invasive and harmful enough, but the leak of information attached to one's name that makes that person susceptible to discriminatory consequences is simply unacceptable. Losing a job or being denied service solely because of one's sexual orientation or gender identity is offensive in any circumstance, but it is unfathomably odious if that were to occur because a healthcare provider had insufficient security protections on their servers.

Until substantive anti-discrimination protections are offered to all LGBTQ people in the United States, gaps in this population's constitutional rights must be protected by all legally available means. A great lapse in justice is avoidable, but only if changes are made quickly.

The potential connection between LGBTQ discrimination and health data breaches exists. The solutions presented here are preliminary suggestions; significantly more study should occur on this topic. Animus-driven data breaches have only just begun; Hzone and Ashley Madison were early warning shots. The costs are worth it, and LGBTQ people along with the rest of the United States deserve better protection of their personal data.