Journal of Health Care Law and Policy

Volume 24 | Issue 2 Article 4

HIPAA, Katz, and the Privacy Gap

Ryan L. Paukert

HIPAA, KATZ, AND THE PRIVACY GAP

RYAN L. PAUKERT*

*"Relying on the government to protect your privacy is like asking a peeping tom to install your window blinds." - John Perry Barlow***

I. INTRODUCTION

Recently while observing court proceedings, I saw a woman opposing a petition ordering electro-convulsion therapy to treat her schizophrenia. The petitioner, the woman's current medical treatment center, noted that previous treatments had proven ineffective and discussed the success rate of electro-convulsion therapy. Later, the woman was put on the stand to testify, answering many questions about her medical history, previous experiences with electro-convulsion therapy from her childhood, and her reasons for refusing the treatment now. Additionally, a court-appointed psychological examiner gave the court his opinion regarding the woman's schizophrenia and the likelihood of success for electro-convulsion therapy in treating her specific conditions. While this situation raises fascinating issues regarding the morality and consequences of compelled treatment, what disturbed me the most was that I, a random member of the public, was able to "listen in" on this sensitive information regarding this woman's medical history and treatment at a public proceeding.

We normally think of privacy in terms of reasonable expectations. This mindset leads to situations in which much information is unprotected because in a modern, technologically advanced society, people cannot reasonably believe

*J.D. University of St. Thomas School of Law (Minnesota), 2020; B.S. University of Wisconsin-Madison, 2012. Thank you to my parents and siblings for supporting me in all my endeavors and to Professor Robert Kahn for his encouragement and teaching me to write like a lawyer. I also want to thank the staff of the University of Maryland *Journal of Health Care Law and Policy* for their careful editing of this Article.

** John Perry Barlow, *Decrypting the Puzzle Palace*, COMM. OF THE ACM (Jul. 1992) http://groups.csail.mit.edu/mac/classes/6.805/articles/digital-telephony/Barlow_decrypting_puzzle_palace.html.

their information will remain private.[1] Yet, when it comes to protected health information ("PHI") covered by the Health Insurance Portability and Accountability Act ("HIPAA"), we take a different, absolutist approach to privacy. The diverging interpretations of privacy based on the involved parties creates a gray area among the general public as to what information is private and what alleged violations are actionable. I refer to this ambiguity as the "Privacy Gap." This Privacy Gap, which is strongly evident in the Katz Test and HIPAA, should be clarified and reduced by creating a uniform system, or test, for privacy rights.[2] In this paper, I will discuss three questions: (1) Can the absolute protection of PHI in HIPAA be reconciled with the Katz Test's notion of a "reasonable expectation of privacy?"[3]; (2) If HIPAA and Katz are irreconcilable, does it matter?[4]; and (3) Assuming HIPAA and Katz are indeed irreconcilable and this is a problem, how should this be resolved?[5]

Part II will explore differing views of privacy, particularly whether privacy ought to be protected and whether individuals should be able to offer their private information as a marketable commodity.[6] This discussion will serve as a backdrop for interpreting the discrepancy in privacy across the board, particularly with a look toward personal health information. In Part III, I discuss the Reasonable Expectation of Privacy Test (Katz Test), with an emphasis on how it applies, or could apply, to medical information that is not covered by HIPAA.[7]

Part IV turns to HIPAA, which protects PHI related to healthcare and insurance regardless of any expectation of privacy.[8] In the process, HIPAA protects at least some information that would be without protection under Katz and the amount of this exposed information will only increase as society becomes more accepting of public displays of sensitive information.

Part V discusses possible explanations for this discrepancy.[9] The reasons include the sensitivity of PHI and possible ramifications of disclosure as well as the nature of HIPAA as a statute, which inherently provides more protection than

1. For example, through the use of social media, the actions and involvement of individuals may be observed by non-present third parties, regardless of these individuals' own participation in social networks.

2. The Katz Test, discussed *infra* Part III, creates a framework for courts to determine whether a person has a constitutionally protected expectation of privacy. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

3. *See infra* Parts II, III, IV.

4. *See infra* Part V.

5. *See infra* Part VI.

6. *See infra* Part II.

7. *See infra* Part III.

8. *See infra* Part IV.

9. *See infra* Part V.

the Fourth Amendment requires.[10] If, as I suggest, this discrepancy is irreconcilable, Part VI reviews possible solutions to close the Privacy Gap between HIPAA and Katz, including revising the Katz Test to grant "unexpected" protections on privacy or, if society determines that privacy is not sufficiently valuable, eliminating HIPAA.[11] In the conclusion, I will address health privacy's current status and other possible issues that may need to be addressed.[12]

II. PRIVACY PERSPECTIVES APPLIED TO PERSONAL HEALTH INFORMATION

Many legal scholars have analyzed the concept of privacy over the years and there is no shortage of diverse viewpoints. Two of the greatest contentions are defining the purpose of privacy and determining how much value should be attributed to it as opposed to conflicting ideals. The following three opinions take profoundly different approaches to privacy. These viewpoints will set the stage for the remainder of the article and addressing the Privacy Gap as well as explore how differing minds might value privacy.

A. Anita Allen's Paternalistic Approach to Privacy

In Anita Allen's article, *Coercing Privacy*, she discusses the liberal conception of privacy, which is the "idea that government ought to respect and protect interests in physical, informational, and proprietary privacy."[13] While she acknowledges that privacy can enable oppressive behavior, such as domestic violence, to go unnoticed and unpunished, Allen offers the position that it may be necessary to restrict an individual's ability to disseminate personal information to safeguard his or her privacy. "[M]aybe we should be prepared to force people to have private lives and to live their private lives in private. Not, as in the past, so they can be kept in their place, but so that they can reap the full dignitarian and political consequences of privacy."[14] Allen argues that the primary goal of privacy should be empowering individuals to live their lives in whatever way they choose, but by allowing these same individuals to release any information about themselves would be self-defeating.[15]

Perhaps there is something to be said for this paternalistic take on privacy, especially within the realm of personal health information, by preventing individuals from releasing sensitive, and possibly damaging, information about themselves. Consider Project Semicolon, a nonprofit based out of Colorado

10. *See infra* Part V.

11. *See infra* Part VI.

12. *See infra* Part VII. As a caveat, this paper is primarily meant to identify the "Privacy Gap" and the need to close it, while how the gap is closed is only secondary.

13. Anita L. Allen, *Coercing Privacy*, 40 WM. & MARY L. REV. 723, 723 (1999).

14. *Id.* at 752.

15. *Id.* at 752–53.

which works toward suicide prevention through education and awareness.[16] Founded in 2013, Project Semicolon gained quick recognition and a substantial following, with many of its supporters getting tattoos of a semicolon, frequently on their wrists, to remove the stigma of mental illness.[17] While this movement is certainly a noble cause, failing to recognize the risk of discrimination to these individuals as a product of this tattoo would be unwise.

Allen's position on privacy would certainly endorse the concept of empowering individuals to live their lives "out in the open," but she might also pause before affirming an individual's choice to get a semicolon tattoo. Mental health information can have a significant impact on an individual's ability to gain employment or even enter new relationships. The average human resources department would not encourage applicants to include their political affiliation or religious denomination on a job application.[18] In that same vein, walking into a job interview with a semicolon tattoo on the wrist, paired with the tattoo's current notoriety, would likely diminish the applicant's chance of getting hired. While the Americans with Disabilities Act outlaws discrimination related to mental health in hiring practices,[19] the presence of a semicolon tattoo could be the factor that decides between two equally qualified candidates. This may be the type of situation where Allen would affirm the government forcing people to "live their private lives in private."[20]

B. Richard Posner's Case for Prying into Private Information

Not all legal scholars share Allen's view that privacy is a good to which all individuals are entitled (and the greater overall personal freedom that comes with it). Richard Posner takes an economic approach to privacy in his article, *The Right of Privacy*.[21] Posner evaluates privacy in conjunction with "prying," which enables an individual to "form a more accurate picture of a friend or colleague."[22] By guarding their private information, people attempt to "manipulate by misrepresentation other people's opinion of them."[23] Posner brings to light that,

16. *About the Project*, PROJECT SEMICOLON, https://projectsemicolon.com/about-project-semicolon/ (last visited Dec. 31, 2019).

17. Doug Bolton, *People All Over the World are Getting Semicolon Tattoos to Draw Attention to Mental Health*, INDEPENDENT (July 4, 2015), https://www.independent.co.uk/life-style/health-and-families/people-all-over-the-world-are-getting-semicolon-tattoos-to-draw-attention-to-mental-health-10365313.html.

18. Alison Doyle, *Top 15 Things You Can Leave Off Your Resume*, THE BALANCE CAREERS, https://www.thebalancecareers.com/top-things-not-to-include-in-a-resume-2063132 (last updated Oct. 2, 2019).

19. EQUAL EMP. OPPORTUNITY COMM'N, YOUR EMPLOYMENT RIGHTS AS AN INDIVIDUAL WITH A DISABILITY (1992).

20. *See supra* note 15.

21. Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 393 (1978).

22. *Id.* at 395.

23. *Id.*

although individuals have a justified interest in their privacy, others have a similarly legitimate interest in discovering that hidden information.[24] "A seldom-remarked corollary to a right to misrepresent one's character is that others have a legitimate interest in unmasking the deception."[25]

When viewed from a health information lens, Posner would not back down from his stance; he even mentions medical data in the article: "Other private information that people wish to conceal, while not strictly discreditable, would if revealed correct misapprehensions that the individual is trying to exploit, as when a worker conceals a serious health problem from his employer or a prospective husband conceals his sterility from his fiancée."[26] The worker and potential husband are both trying to sell themselves as something other than what is the full truth. Posner suggests that an individual's medical information could not only correct misapprehensions but may very well be necessary for the other party's decision-making. Just as there are laws requiring sellers to disclose information about homes to potential buyers,[27] Posner argues that people have a right to similar disclosures about their neighbors, colleagues, and friends.[28]

In the context of the semicolon tattoos, Posner would diverge from Allen's protectionist view of privacy, arguing instead that employers and other acquaintances should be able to pry and factor in this accessible information when making important decisions about these individuals.[29] But, more than that, they have a right to know. "We think it wrong (and inefficient) that the law should permit a seller in hawking his wares to make false or incomplete representations as to their quality. But people 'sell' themselves as well as their goods."[30] Hence, Posner would argue if an individual's mental condition is a legitimate issue, those that associate with him or her should be able to use available means to discover it.[31] Posner summarizes the issue best by asking, "[w]hy should others be asked to take their self-serving claims at face value and be prevented from obtaining the information necessary to verify or disprove these claims?"[32]

24. *See id.*

25. *Id.*

26. *Id.* at 399.

27. *Required Disclosures When Selling U.S. Real Estate*, NOLO, https://www.nolo.com/legal-encyclopedia/required-disclosures-selling-real-estate-30027.html (last visited Dec. 31, 2019).

28. Posner, *supra* note 21, at 399.

29. *Id.*

30. *Id.*

31. *Id.* at 400.

32. *Id.*

C. Spiros Simitis's Warning of Partial Information

This final perspective provided by Spiros Simitis in *Reviewing Privacy in an Information Society*, specifically examines privacy from the perspective of emerging technology, which is highly relevant for health information in the digital age.[33] Simitis acknowledges the ambiguity that has followed the term "privacy" as commentators have tried to define it, noting "the more the need for a convincing definition of privacy based on criteria free of inconsistencies has been stressed, the more abstract the language has grown."[34] Rather than attempt to define privacy when so many others have failed, Simitis instead focuses on how current forms of data collection have "altered the privacy discussion."[35] The digital collection of health information greatly affects the public, especially when the collected private information does not paint the full picture.

The collection of health information has many benefits, some of which lie with insurance companies. Insurance companies attempt to understand which services and medical care their patients most need.[36] By understanding common health problems and the behavior of its clients, an insurance company can tailor health plans that best serve patients while also saving the company (and patients) money. Although an automated system of collecting health information to quickly and efficiently determine which services to provide may usually be helpful, it can also have negative, unintended consequences in complex cases.[37] Simitis discusses an incident where an "elderly woman living in a Massachusetts nursing home" had her benefits terminated because "according to a computer match of welfare rolls and bank accounts, her account exceeded the Medicaid asset limit."[38] However, the computer did not recognize that a certificate of deposit in her account was an exempt resource under federal regulations and should not have been included in the "calculation of her assets for purposes of Medicaid."[39]

While the automated collection of personal health information is valuable in that it removes any potential biases that are attached to human minds while adding greater speed to the process, it is also damaging for that same reason. Humans can look at the full spectrum of facts and apply common sense to them,

33. Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707, 708 (1987).

34. *Id.* at 708.

35. *See id.* at 709 (explaining that modern data collection has changed the privacy discussion in the following ways: "privacy considerations no longer arise out of particular individual problems"; "smart cards and videotex make it possible to record and reconstruct individual activities in minute detail" and; "person information is increasingly used to enforce standards of behavior.").

36. *Health Insurance: Understanding What It Covers*, FAMILYDOCTOR.ORG, https://familydoctor.org/health-insurance-understanding-covers/ (last visited Feb. 9, 2018).

37. *See infra* notes 38–39.

38. Simitis, *supra* note 33, at 718.

39. *Id.* at 718–19.

a capability that machines do not yet have. One consequence of automated processing that Simitis raises is the "loss of context."[40] Returning to the example of the semicolon tattoo, while a computer system might only tell an employer or doctor that an applicant or patient has a history of a particular mental illness, an individual interaction could shed more light. Perhaps this person only had a brief, one-time episode that should have no bearing on medical treatment or her ability to carry out job responsibilities. Here, Posner's concept of "prying" would actually benefit individuals, protecting them from flawed data-collection systems that could withhold benefits to which they would otherwise be entitled.[41]

Upon reviewing the views of Anita Allen, Richard Posner, and Spiros Simitis, there is debate as to the societal value of privacy. "[T]he boundary between a permissible exchange of facts about people, necessary to avoid misrepresentation, and an impermissible intrusion and surveillance is entirely unclear."[42] While Posner asks what information individuals are trying to hide, Simitis questions what relevant information is not being discovered by automated systems, and Allen challenges whether these facts should be accessible at all.[43] Opposing viewpoints of privacy are expressed further by the different manifestations of privacy within different areas of law.

III. KATZ, HEALTH PRIVACY, AND TECHNOLOGY

An older woman is walking down the beach on an overcast day. She begins by telling viewers "[y]ou always wonder…who does make you who you are."[44] Inspirational piano music begins playing as she explains that she was adopted and searched for her birth family for forty years.[45] By using 23andMe.com, however, she was finally able to put that journey to an end. The commercial closes with a touching reunion at the airport and a birthday cake.[46] While this is certainly a beautiful story, the commercial fails to point out that this woman's genetic information is now within the control of a private corporation, which is not subject to the regulations of HIPAA nor the privacy protections of the U.S. Constitution.

The concurring opinion of Justice Harlan in *Katz v. United States* in 1967 created the Reasonable Expectation of Privacy Test, also known as the Katz Test, to rule on Fourth Amendment claims.[47] This test has two prongs for a valid claim

40. *Id.* at 718.

41. Posner, *supra* note 21.

42. Simitis, *supra* note 33, at 709.

43. *Compare* Posner, *supra* note 21, *with* Simitis, *supra* note 33.

44. 23andMe, *Story: 76-year-old Woman Finds Her Birth Family*, YOUTUBE (Oct. 21, 2015), https://www.youtube.com/watch?v=4Ech2cwz9I4.

45. *Id.*

46. *Id.*

47. Katz v. United States., 389 U.S. 347, 361–62 (1967) (Harlan, J., concurring).

of privacy against the government: (1) a person must exhibit an "actual (subjective) expectation of privacy" and (2) the expectation must be one that "society is prepared to recognize as 'reasonable."[48] The Katz Test is frequently used, and perhaps primarily, in criminal cases that involve new technologies, such as thermal detection scanners used to locate residences utilized as greenhouses to illegally grow marijuana or wiretapping, as in the Katz Test's namesake.[49]

The Katz Test, although originating in a criminal case, may have a limited application to medical information that does not fall under the umbrella of PHI, but these instances are rare since the Katz Test only applies to the government.[50] Protected Health Information is any information, whether oral or recorded in any form or medium, that (1) "is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse" and (2) "relates to the past, present, or future physical or mental health or condition of any individual, the provision of healthcare to an individual."[51] Additionally, PHI must be information that "identifies the individual" or creates a "reasonable basis to believe the information can be used to identify the individual."[52] This definition leaves a large portion of an individual's health information unprotected by HIPAA and the Katz Test fails to sufficiently pick up the slack since it can only hold the government accountable for privacy violations.

Under the first prong, any medical information that is created or received by a party other than those listed is not protected. Therefore, any government agency or office that does not meet one of those definitions is not subject to HIPAA.[53] Yet, even if the government were to meet the HIPAA requirement, legislators saw fit to provide a laundry list of exceptions to HIPAA's applicability, many of which benefit the government.[54] As explained in the introduction, the government exposed a great deal of personal health information about a schizophrenic woman in public court, but there was no HIPAA violation

48. *Id.* at 361.

49. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 40 (2001) (holding that the use of technology that is not in general public use to "intrude" on a private home was presumptively unreasonable).

50. *Katz*, 389 U.S. at 361–62.

51. 45 C.F.R. § 160.130 (2021).

52. *Id.*

53. *See supra* notes 51–52 and accompanying text (explaining what sort of information is protected by HIPAA).

54. *See generally* 45 C.F.R. § 164.512 (2021) (exempting law enforcement, public health authorities, the military, and other covered entities from HIPAA obligations in certain circumstances involving, for example, licensure actions, criminal investigations, matters of national security, oversight of the health care system, and administration of government benefit programs).

since disclosure during "judicial or administrative proceeding" is one of HIPAA's many exceptions.[55]

Polls typically show that Americans strongly favor laws that will protect their privacy.[56] A 2008 Pew research poll found that 90% of respondents "would be very concerned if the company at which their data were stored sold it to another party" and 80% said "they would be very concerned if companies used their photos or other data in marketing campaigns."[57] However, polls also show that many Americans feel the need to adjust security settings on social media to increase their privacy.[58] The conundrum with this factor is that increasing privacy settings indicates that these people did not believe their information was being protected to begin with, otherwise they would not have felt the need to increase the privacy settings (although the argument could be made that by increasing security settings, an individual demonstrates his desire to protect privacy). This conclusion is supported by a Pew research poll revealing that Americans lacked confidence that their private information, particularly online, would actually stay private.[59]

IV. THE ABSOLUTIST PROTECTION OF PRIVACY UNDER HIPAA

Unlike the Katz Test's subjective approach to privacy, HIPAA takes an objective stance. HIPAA guards an individual's "Protected Health Information."[60] Additionally, to qualify as PHI, the information must be of the kind that "identifies the individual" or generates a "reasonable basis to believe the information can be used to identify the individual."[61]

Many benefits exist in HIPAA that would be eliminated if the Katz Test had been adopted for medical information instead. The first prong of the Katz Test would be difficult to meet for many patients. Individuals with Type 1 Diabetes typically wear an insulin pump on their waists to treat their condition.[62] Under Katz, these patients would lack a reasonable expectation of privacy in this condition since these pumps are noticeable to the general public.[63] Further, the

55. *Id.* § 164.512(e).

56. *Public Opinion on Privacy*, ELEC. PRIV. INFO. CTR., https://epic.org/privacy/survey/ (last visited May 15, 2019).

57. *Id.*

58. *Social Networking Privacy*, ELEC. PRIV. INFO. CTR., https://epic.org/privacy/socialnet/ (last visited May 15, 2019).

59. Mary Madden & Lee Rainie, *Americans' Attitudes About Privacy, Security and Surveillance*, PEW RSCH. CTR. (May 20, 2015), https://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/.

60. 45 C.F.R. § 160.103 (2021).

61. *Id.*

62. *Type 1 Diabetes*, MAYO CLINIC (Aug. 22, 2020), https://www.mayoclinic.org/diseases-conditions/type-1-diabetes/diagnosis-treatment/drc-20353017.

63. *See* Katz v. United States., 389 U.S. 347 (1967) (Harlan, J., concurring).

second prong of Katz asks whether the expectation is one which society is prepared to recognize as "reasonable."[64] The difficulty lies in the general public's unawareness of what medical information ought to be protected. For example, the general public may be unaware of the ramifications of certain medical conditions being known by potential employers.

While HIPAA protects a large amount of health information, there is a great deal of personal medical information that is left unsheltered. A cybersecurity consultant in Florida purchased an at-home paternity test to try out with her family, curious to see how the system worked.[65] After mailing it in, she went on the company's website to see the results, but by slightly altering the website's URL, a "sprawling directory appeared that gave her access to the test results of some 6,000 other people."[66] The consultant reported this "seemingly obvious violation of patient privacy" to the Department of Health and Human Services, but was shocked to discover that officials could not do anything since at-home paternity test companies are not subject to HIPAA.[67]

In a world of social media, digital apps, and fitness data tracking devices, many individuals are freely sharing information about themselves to the world that compromises their health privacy, whether they realize it or not. One of the best examples of this is the Fitbit, a device that is worn as a wristwatch and synchronizes through Bluetooth with a smartphone app.[68] While most people only think of a Fitbit as tracking an individual's accumulated steps throughout the day, these fitness trackers can do much more.[69] The Versa, one of Fitbit's high-end models, tracks the following information without any affirmative actions by the user: steps via GPS, sleep, heartrate, calories burned, activity types, and duration of activity.[70] Additionally, the user can log the following information in the free Fitbit app: calories consumed, weight, water intake, and female health.[71] Few family doctors have access to this much information about

64. *Id.* at 361.

65. Charles Ornstein, *Privacy Not Included: Federal Law Lags Way Behind New Healthcare Technology*, PAC. STANDARD (Jun. 14, 2017), https://psmag.com/social-justice/privacy-not-included-federal-law-lags-way-behind-new-health-care-technology.

66. *Id.*

67. *Id.*

68. *See generally* FITBIT, https://www.fitbit.com/about (last visited May 15, 2019) (showing images of Fitbit wristwatch devices for sale that can be linked to smartphone apps via Bluetooth, as well as screenshots for those apps).

69. *See id.*

70. *Let's Talk About Privacy*, FITBIT, https://www.fitbit.com/global/us/legal/privacy-summary (last visited May 15, 2019).

71. FITBIT, *supra* note 68.

their patients, and yet, this information is not protected by HIPAA since Fitbit is not a covered entity.[72]

Personal fitness trackers are not the only area of medical information that HIPAA does not reach. DNA-testing corporations, such as Ancestry.com and 23andMe, have recently surged in popularity.[73] For $100, consumers can receive a DNA testing kit, requiring only a saliva sample, and return it to the respective company for a genetic report, including "health predispositions" and "carrier status."[74] This information relates to "past, present, [and] future" physical health, yet HIPAA does not apply since these corporations are not covered entities.[75]

Despite the previously stated detriments of a Katz Test for health information, a similar subjective privacy test would likely subject companies like Fitbit and 23andMe to civil and criminal penalties for releasing or selling health information that HIPAA does not. People likely believe their weight and caloric intake data entered in the Fitbit app will never leave the safety of their smartphones. A son that gifts a DNA test to his mother to show "what makes her so special" likely does not anticipate that completing the test now makes her genetic report – and consequently his genetics – a commodity of Ancestry.com.[76] Further, society as a whole would likely find these to be acceptable privacy expectations of companies dealing in health information. Therefore, while HIPAA's current language would not protect this data, a medical version of the Katz Test applicable to private parties could keep this information safe.

While there is still the danger of the Katz Test losing its effectiveness as Americans relinquish their expectation of privacy, some polls show that this may not be for some time, at least for their medical data. A 2016 Pew research poll found that after social security numbers, Americans were most sensitive regarding their state of health and medications they take.[77] Although privacy concerns about buying habits and media consumption are practically extinguished, health privacy is still greatly valued, but for how much longer is uncertain.[78]

72. *See* DEP'T HEALTH & HUMAN SERVS., *Covered Entities and Business Associates*, (Jun. 16, 2017) https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html (explaining that a covered entity is either (1) a health care provider, (2) a health plan, or (3) a health care clearinghouse).

73. Amy Brown, *DNA Testing Is Popular, But Many are Unaware of Privacy Concerns*, TRIPLE PUNDIT (Dec. 18, 2018), https://www.triplepundit.com/story/2018/dna-testing-popular-many-are-unaware-privacy-concerns/55936.

74. 23ANDME, https://www.23andme.com/dna-health-ancestry/ (last visited May 15, 2019).

75. *Id.*

76. ANCESTRY.COM, https://www.ancestry.com/dna/?o_iid=98455&o_lid=98455&o_sch=Web+Property (last visited May 13, 2019).

77. *The State of Privacy in Post-Snowden America*, PEW RSCH. CTR. (Sept. 21, 2016), https://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/.

78. *Id.*

The development of algorithms in data analytics will compromise health privacy and further extend the Privacy Gap between what HIPAA actually protects and information that will soon be accessible by new algorithms. The JAMA Network conducted a study to reveal the feasibility of reidentifying individuals based on a small sample of their physical activity and some demographics, including age, sex, ethnicity, and education.[79] Using a "support vector machine," researchers were able to re-identify individuals with 95% accuracy by comparing a sample of their identified health data to anonymous data that was collected later.[80] This technology greatly impacts HIPAA since health information will become increasingly difficult to "de-identify" from the individual that produced it.[81] This will place an even greater burden on HIPAA entities to protect data, while those entities not covered will gain access to additional information connecting current data to health information that was released while the data was still thought to be "de-identified" pursuant to HIPAA. This means, HIPAA entities would be subject to a massive responsibility in protecting patient information, while commercial corporations will in theory be able to run rampant with the data they collect.

While the Katz Test was a workable solution back in 1967, the year of its creation, the diminishment of subjective expectations of privacy have gradually worn away its utility.[82] Meanwhile, although HIPAA applies to the most mainstream possessors of medical data, its inability to reach uncovered entities makes it a rigid law that fails to serve the ideal purpose of protecting sensitive health information. Neither the Katz Test nor HIPAA is a perfect solution to protecting health data but understanding the two approaches may allow legislators and constituents to make appropriate changes going forward.

V. WHY HIPAA GOES BEYOND KATZ

HIPAA offers significantly greater protections for health information than the Katz Test does for privacy violations by the government. While the Katz Test creates a wide net that allows certain privacy violations by the government to slip through, HIPAA erected an unyielding wall around entities subjected to its

79. Liangyan Na et al., *Feasibility of Reidentifying Individuals in Large National Physical Activity Data Sets from Which Protected Health Information Has Been Removed with Use of Machine Learning*, JAMA NETWORK 4–5 (Dec. 18, 2018), https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2719130.

80. *Id.* at 1.

81. *See generally* DEP'T HEALTH & HUMAN SERVS., GUIDANCE REGARDING METHODS FOR DE-IDENTIFICATION OF PROTECTED HEALTH INFORMATION IN ACCORDANCE WITH THE HEALTH INSURANCE AND PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) PRIVACY RULE (Nov. 26, 2021) https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf (providing guidance regarding the de-identification of PHI).

82. *See* Katz v. United States, 389 U.S. 347 (1967) (noting the Supreme Court's establishment of the *Katz* test when evaluating Forth Amendment claims).

rule (e.g., hospitals and insurance providers).[83] These differences have helped create the Privacy Gap that puts citizens at a disadvantage when determining their privacy rights and expectations. This system of privacy creates confusion among the public, but there are a few possible explanations for this inconsistency.

The first, and possibly most cynical, explanation is that the government wants to reduce their potential liability, but is indifferent to the liability of private parties, such as hospitals and other medical providers. HIPAA targets the medical field, while the Katz Test targets the government, the very entity that created the different privacy standards. Although there are HIPAA entities that are state-run, such as universities and public hospitals, the vast majority are private. According to statistics by the American Hospital Association in 2013, of the 5,724 hospitals in the United States, only 1,045 were owned by the government, less than 20 percent.[84] Yet, the government can still obtain medical records through the Patriot Act and a Foreign Intelligence Surveillance Act ("FISA") warrant.[85] While the Katz Test was created in a concurring opinion by the Supreme Court, legislators can overcome these judicial tests by creating laws to resolve the ambiguities that existed when the Court first heard the case.[86] Those in the medical profession are left to rely on lobbying groups with little ability to effect direct change on their own. Few would be surprised that the government would set a higher standard for private corporations than for itself when it comes to legal liability. After all, the government is only subject to lawsuits when it chooses to be.[87]

A second possible reason for the discrepancy is that, while the subjective privacy standard found in the Katz Test is good enough for holding the government accountable, it is insufficient for PHI and healthcare organizations. The Katz Test is used to execute the right to privacy in the Fourth Amendment of the Constitution.[88] Constitutional rights are only applicable to violations made by the federal or state governments. Further, since the government is the alleged violator, there are many more claims available due to the Constitution and the rights it provides than those available against private parties that violate privacy. Additionally, of all the information that Americans consider private, medical

83. *See* DEP'T HEALTH & HUMAN SERVS., *supra* note 72 (explaining covered entities and business associates that are subject to the HIPAA Privacy Rule).

84. *50 Things to Know About the Hospital Industry*, BECKERS HOSPITAL REV. (2013).

85. *FAQ on Government Access to Medical Records*, AM. CIV. LIBERTIES UNION, https://www.aclu.org/other/faq-government-access-medical-records (last visited May 15, 2019).

86. *See* Katz v. United States, 389 U.S. 347 (1967) (noting the Supreme Court's establishment of the *Katz* test when evaluating Forth Amendment claims).

87. *Sovereign Immunity*, LEGAL INFO. INST. (Dec. 31, 2019), https://www.law.cornell.edu/wex/sovereign_immunity.

88. U.S. CONST. amend. IV.

data is one of the most sensitive.[89] Due to the high value placed on PHI, the creation of a higher standard is understandable. Yet, the question remains as to why the government would not err on the side of caution and place a high standard for all private information, regardless of how much Americans value the different types.

A final, more optimistic, potential reason for the Privacy Gap is the government desiring to protect its people from themselves, much in the vein of Anita Allen's hopes discussed above.[90] In all fairness, this is a perfectly understandable reason. We live in an age where citizens can simultaneously be too young to vote yet also reveal information about themselves to the world with the tap of a button – information that can be used against them throughout their lives. Minors with a reduced understanding of the long-term consequences of their actions may need to be protected from themselves. But should the government take this paternalistic approach? And if so, is HIPAA the proper solution for safeguarding health information? Although Katz is a subjective test, Americans are guaranteed a slew of remedies under the Constitution – remedies which are unavailable when the alleged violator is another private party. Perhaps the government is merely attempting to place these HIPAA entities at a higher level of responsibility, closer to that of the government, because an individual's health information is that important. But this conclusion begs the question: Will exposure of our medical information actually have detrimental effects on us?

People go to hospitals for a variety of reasons, but only some of these reasons would be considered sensitive or confidential. Few people would suggest that receiving a flu shot or attending a regular checkup need to be shielded from prying eyes. However, other pieces of delicate medical information could be used against individuals if released to the public. A current controversy is parents' decisions to not vaccinate their children. Many parents ban unvaccinated minors from playing with their own children once they discover this medical information.[91] Similar discrimination would arise elsewhere. Engineers and doctors need to distinguish between different colors in their work and a diagnosis of colorblindness could be a bar to entrance into college programs or an obstacle to future employment.[92] Dating could become an insurmountable challenge if an

89. *See The State of Privacy in Post-Snowden America*, *supra* note 77 (referencing a 2016 Pew Research poll finding that Americans are sensitive regarding the state medical information).

90. *See supra* Section II.a. (focusing on Anita Allen's paternalistic approach to privacy).

91. Elizabeth Whitman, *Anti-Vaccine Movement Scares Parents Trying to Set Up Playdates: How to Ask About a Child's Vaccination History*, INT'L BUS. TIMES (Feb. 23, 2015, 3:29 PM), https://www.ibtimes.com/anti-vaccine-movement-scares-parents-trying-set-playdates-how-ask-about-childs-1803952.

92. *See* Jason McDowell, *When Color Blindness Gets in the Way of Your Career Dreams*, RECRUITER (Mar. 3, 2017), https://www.recruiter.com/i/when-color-blindness-gets-in-the-way-of-your-career-dreams/ (explaining how a diagnosis of color blindness can negatively impact professional careers in various industries).

individual's infertility or disease carrier status were as discoverable as their musical interests. Private schools may be unwilling, or at least hesitant, to accept students diagnosed with learning disabilities. Further, these forms of discrimination could even extend to distant ancestors, regardless of any relevance to modern times.

In *Finding Your Roots*, a PBS genealogy program, celebrities are given the opportunity to have expert genealogists dive into their origins, discovering their family's history along the way.[93] While many of the show's featured guests received interesting and harmless pieces of ancestral trivia, others learned embarrassing, and even controversial, family secrets.[94] One such celebrity was Ben Affleck, an American actor and producer.[95] Affleck discovered, much to his displeasure, that one of his ancestors was a slaveowner.[96] While the majority of people would be ashamed to find this piece of fruit on their family tree, the real controversy was Affleck's attempt to hide this information from the American public.[97] Affleck was able to dissuade PBS from airing that particular segment of his episode, which was later discovered via Wikileaks.[98] Although an individual's distant ancestors contribute little to the values and morals of the present-day descendants, the fear of a distorted image is very real.

The negative consequences of exposed medical data would likely extend beyond rational reasons. Real estate transactions could become complicated by a seller or potential buyer's HIV/AIDS status. Potential buyers may be hesitant to purchase a property that was previously inhabited by an HIV positive individual, despite the lack of any real adverse effects on the property, or sellers may feel pressure from neighbors to not sell for similar concerns about potential buyers. Employers could even be reluctant to hire someone with a genetic predisposition for a condition that may not even hamper their ability to do the work. This list is only a few of the possible ramifications of exposed PHI. Returning to Affleck's situation above, although it does not deal with PHI, the scenario and potential ramifications are comparable. The most disturbing aspect to that entire saga is that Affleck was persecuted for trying to keep personal information about himself, and his family, private. At what point in the future will individuals be criticized for trying to withhold their family's history of heart disease or diabetes?

93. Sarah Kaplan, *After Omitting Details of Ben Affleck's Slave-owning Ancestor, 'Finding Your Roots' is Suspended by PBS*, WASH. POST (June 25, 2015, 5:03 AM), https://www.washingtonpost.com/news/morning-mix/wp/2015/06/25/after-omitting-details-of-ben-afflecks-slave-owning-ancestor-finding-your-roots-is-suspended-by-pbs/.

94. *Id.*

95. Ben Affleck, IMDB.COM, https://www.imdb.com/name/nm0000255/?ref_=nv_sr_2?ref_=nv_sr_2 (last visited Dec. 30, 2019).

96. Kaplan, *supra* note 93.

97. *Id.*

98. *Id.*

HIPAA was created, at least in part, to provide peace of mind to patients by laying out heavy penalties on covered entities for violating the statute.[99] While HIPAA protects additional information that would be vulnerable under a subjective test like Katz, there is also a certain degree of extrinsic harm that comes with the statute. People would surely like to know what information is private and what remedies are available for a breach of that information, but until some uniform understanding of "privacy" is adopted they will be left to guess. An unfortunate result of confusing circumstances like these is inaction by the victims who do not know what their rights are or if they have even been violated. The Privacy Gap needs to either be shrunk or bridged so average Americans can understand their rights to privacy and properly exercise them.

VI. BRINGING HIPAA AND KATZ IN LINE WITH EACH OTHER

Several possible solutions for closing the Privacy Gap are discussed in this section. While none of them are a panacea for the problem, each discussion will shed some light on the advantages and disadvantages of the respective solution.

A. Eliminate HIPAA and Similar Statutes & Expand the Katz Test

Great unfairness exists between the standards of privacy between state actors and those in the medical profession. The Katz Test's subjective analysis requires the state to owe privacy to individuals, but only when they possess an actual "reasonable expectation" of privacy and that expectation must be acceptable to society at large.[100] As technology continues to advance and personal information becomes more accessible online, any "reasonable expectation" of privacy is gradually eroding away. Granted, the general public, not the government, is primarily responsible for this decline in expectation, but that does not mean the government should be able to pry into sensitive information without consequences.

On the other side is HIPAA, which places an unyielding restraint on medical professionals when handling PHI.[101] All covered entities in the rule are subject to HIPAA and must protect PHI or face huge penalties.[102] But, if a company is lucky enough to not be on the short list of covered entities, it will not be subject to HIPAA despite possessing the same information as covered entities.[103] This result suggests Congress has not seen the need to act quickly

99. *See What Are the Penalties for HIPAA Violations*, HIPAA J. (Jan. 15, 2021), https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/ [hereinafter HIPAA Penalties] (discussing penalties for covered entities in violation of the statute).

100. *See* Katz v. United States., 389 U.S. 347 (1967) (noting the two prong Katz Test for a valid claim of privacy infringement against the government).

101. *See supra* Part IV (referencing the absolutist protection of privacy under HIPAA).

102. *See* HIPAA Penalties, *supra* note 99 (explaining penalties for HIPAA Privacy Rule violations).

103. 45 C.F.R. § 160.130(1)–(3) (2014).

with regard to PHI or is simply more concerned with punishing negligent hospitals than actually protecting PHI under HIPAA. Additionally, under HIPAA, PHI must be protected if it can identify specific individuals.[104] As explained, programs and algorithms are in development which allow de-identified individuals to be re-identified and the amount of information needed to complete the task lessens every day. Therefore, while the state benefits from advancements in technology, medical providers are forced to comply with higher and higher standards of privacy protection.

Broadening the Katz Test to apply in all civil and criminal privacy cases would remove a great amount uncertainty regarding PHI, but changes to the test are necessary to adequately guard private information. The most glaring problem with Katz is the subjective expectation of privacy requirement. Perhaps it is a natural change, but people do not have a strong expectation of privacy anymore.[105] A possible solution would involve adopting a modified version of the "Third Party Doctrine," which states "information loses Fourth Amendment protection when it is knowingly revealed to a third party."[106] The greatest benefit to this doctrine is the mens rea requirement of "knowingly" revealing the information. Many people give information to entities, like hospitals and smartphone apps, but they would be reticent to say they knowingly revealed the information. The modification would be to create a list of third-party exceptions, where despite a knowing reveal, the information would retain its private nature. The list could include immediate family, close personal contacts, etc. An additional, capitalistic benefit to this solution is it would allow individuals to freely sell their private information to corporations without the corporations being penalized for their use of the data. The contracts would only need to have a "knowingly reveal" clause to prevent any possible privacy claims later on.

However, at least one problem exists with this solution; the Third Party Doctrine has been accused of being the Katz Test in disguise since a knowing revelation to a third party would basically equate lacking a "reasonable expectation of privacy." As such, modifications would be necessary.

B. Create More Statutes Like HIPAA and Retain the Katz Test as a Residual Net

If the government's goal is truly protecting an individual's private information as much as possible, then not only should legislators create more statutes like HIPAA, but Congress should implement the Katz Test as a last line

104. *See* DEP'T HEALTH & HUMAN SERVS., *supra* note 81, at 5 (explaining that the process of de-identification "mitigates privacy risks to individuals).

105. *See, e.g.*, Derek M. Alphran, *Changing Tides: A Lesser Expectation of Privacy in a Post 9/11 World*, 13 RICH. J.L. & PUB. INT. 89. 90 (2009) (explaining how the Supreme Court's interpretation of the Fourth Amendment evolves with society's changing views on privacy).

106. Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009).

of defense for information that is not explicitly protected by statute. Not only would objective tests like HIPAA enforce strict compliance by the covered entities, but the supplemental Katz Test would prevent non-covered entities, like Ancestry.com and Fitbit, from escaping penalties due to Congress failing to contemplate them at the time of drafting. By asking whether the individuals had a reasonable expectation of privacy when they gave the information to the non-covered entity, individuals will retain a remedy for the violation.

These statutes would function similarly to HIPAA with a basic two prong formula. The first prong would address which entities are covered by the statute, such as employers, social media platforms, or commercial retailers. The second prong would state what information the respective entities would be required to protect. An employer, for example, could be required to protect any work product produced by the employee, past or present, which is legally owned by the employee rather than the employer. Similarly, any financial institutions that maintain the funds of private individuals could be required to guard histories of deposits, withdrawals, and any other pieces of information the legislatures deems worthy of screening.

A likely problem with this solution is the undue hardship it would place on subjected organizations. For employers that have a high rate of turnover, they may need to retain and shield large amounts of data from former workers. A possible fix would be including an expiration clause in employment contracts to relieve an employer of any statutory duty to protect non-sensitive, yet still private, information held by the employer. Further, this solution would still create, and possibly expand, the Privacy Gap. What may be protected information for an entity under one statute may be unprotected by entities subject to a different statute. Congress could try to combat this by compiling all of the statutes into a single chapter of the Code of Federal Regulations, but it could become extremely costly and time-consuming to do so.

C. Eliminate HIPAA and Allow the States to Create Their Own Laws

While HIPAA acknowledges that states can still create their own medical privacy laws, it requires that the laws be "more stringent" than HIPAA to take effect.[107] Yet, states cannot reduce the reach of HIPAA on the covered entities within their borders.[108] Removing HIPAA would enable states to embrace values unique to their medical economy. States like Minnesota, the home of the world-renowned Mayo Clinic,[109] may want to craft statutes more friendly to the medical industry than other states where healthcare is not essential to their economy.

107. 45 C.F.R. § 160.203(b) (2019) (noting that the Federal law preempts State law unless the State's law is "more stringent").

108. *Id.*

109. *Mayo Clinic in Rochester, Minnesota*, MAYO CLINIC, https://www.mayoclinic.org/patient-visitor-guide/minnesota (last visited Mar. 6, 2020).

Further, applying the Katz Test to all areas of privacy would ensure a bare minimum of protection for Americans, but would allow the states to tailor their laws in a way that meets the specific needs of their state.

The biggest issue with this option is its adoption will widen the Privacy Gap if each state decides to do something different. Additionally, intra-state medical treatments would create court problems. Would the laws of the hospital's state or the patient's state control in court? If people knew HIPAA had been repealed, would individuals have an even lesser "reasonable expectation of privacy" than they did before HIPAA's enactment, due to being unaware of state-specific protections? This outcome would defeat the purpose of retaining the Katz Test.

While there is no readily apparent solution to the Privacy Gap, it is worthwhile for lawmakers and their constituents to ask these questions. Technology is not slowing down and if there is any hope of catching up to the privacy problems it creates, we need to act soon.

VII. CONCLUSION

Amazon, the world's largest online retailer,[110] recently announced that Alexa, its virtual assistant, is now HIPAA compliant.[111] People who receive healthcare from one of the six companies that contracted with Amazon to use Alexa for HIPAA-related activities, may now schedule doctor appointments, check their blood sugar levels, etc. all through voice commands given to Alexa.[112] Stephen Cassell, the Senior Vice President of Global Brand and Customer Communications for Cigna, one of the six health companies to contract with Amazon for these new services, had this to say: "…we are meeting customers where they are – in their homes, in their cars – and making it simpler to create healthier habits and daily routines."[113]

Technology is creeping into every corner of our lives – if it has not already – and with this advancement our sensitive data, including our medical records and other PHI, is at our fingertips. Making things easier to do through technology has incredible advantages. People can devote more time to pursue their goals and hobbies with greater ease than ever before, with obstacles minimized or removed completely. But comfort can breed carelessness. This is only one cost of new technology. A child that saves money for a large purchase treats the new item with greater reverence than a child that receives the same as a gift. Perhaps

110. Jessica Young, *Top 10 Online Retailers: How the Largest Online Retailers in the World Fared in 2018*, DIGITAL COMMERCE 360 (Mar. 14, 2019), https://www.digitalcommerce360.com/2019/03/14/top-10-online-retailers/.

111. Rachel Jiang, *Introducing New Alexa Healthcare Skills*, AMAZON (Apr. 4, 2019), https://developer.amazon.com/blogs/alexa/post/ff33dbc7-6cf5-4db8-b203-99144a251a21/introducing-new-alexa-healthcare-skills.

112. *Id.*

113. *Id.*

privacy is just another fee on the price tag of convenience. As Posner argues, "people want to manipulate the world around them by selective disclosure of facts about themselves."[114] By taking advantage of modern conveniences, people assent to prying by third parties, another modern convenience. Perhaps one could even argue that it is better for all health information to be released to avoid inaccurate conclusions, both beneficial and detrimental, being drawn about people.

The end question is not whether medical privacy is important to Americans – polls show that it clearly is[115] – but rather whether HIPAA's true purpose is to protect patients' privacy or punish covered entities for carelessness with PHI. HIPAA fails to adequately protect PHI due to its inapplicability to corporations not covered under the first prong.[116] This limited scope means that the underlying information is not protected, but only that certain entities will be punished for its release. Regardless of Congress' intent while creating HIPAA, the resulting act only provides the illusion that all health information is protected.

Going forward, the fight to protect PHI will not be in doctors' offices and billing statements, but instead on computer screens and phone apps. Currently, the top three most frequent HIPAA violations are unsecured digital records, possessing unencrypted data, and hacking.[117] If we want to protect our privacy in this new age of information, we must know what our rights and remedies are. And this is not a fight we should rely on the government to fight for us. After all, the government wants personal data just as much as private entities, if not more.[118] However, the first step is knowing what privacy means to us as a country. Regardless of the definition chosen for this increasingly abstract term, closing the Privacy Gap and getting the public on the same page is vital to protecting our personal health information.

114. Posner, *supra* note 21, at 400.

115. *See* Madden & Rainie, *supra* note 59.

116. *See supra* Part IV (referencing the absolutist protection of privacy under HIPPA).

117. Kaitlyn Houseman, *Top 10 Most Common HIPAA Violations*, REVELEMD.COM (Dec. 3, 2016), https://www.revelemd.com/blog/top-10-most-common-hipaa-violations.

118. *See generally* Sara Fischer & Scott Rosenberg, *Government Wants Access to Personal Data While It Pushes Privacy*, AXIOS (Aug. 26, 2019), https://www.axios.com/government-wants-access-to-personal-data-while-it-pushes-privacy-aacc15f1-bbcb-481b-b6ae-278e0f15e678.html (explaining how the government uses and benefits from the personal data of its citizens).