SCHOOL OF LAW
CASE WESTERN RESERVE UNIVERSITY

Health Matrix: The Journal of Law-Medicine

Volume 24 | Issue 1

2015

Big Data Proxies and Health Privacy Exceptionalism

Nicolas P. Terry

BIG DATA PROXIES AND HEALTH PRIVACY EXCEPTIONALISM*

Nicolas P. Terry†

[B]ig data . . . is taking advantage of us without our permission. Often without consent or warning, and sometimes in completely surprising ways, big data analysts are tracking our every click and purchase, examining them to determine exactly who we are – establishing our name, good or otherwise – and retaining the information in dossiers that we know nothing about, much less consent to.[1]

CONTENTS

INTRODUCTION 66
I. HEALTH PRIVACY AND "SMALL" DATA 67
A. Understanding the HIPAA Model 67
B. The Maturation of HIPAA 70
C. The Omnibus Rule and Breach Notification 71
II. THE DATA PROXIES' CHALLENGE TO HEALTH PRIVACY 77
A. "Laundered" HIPAA Data 80
B. The Self-Quantified, Self-Curating Patient 82
C. Medically Inflected Data 84
III. HOW "STICKY" IS HEALTH PRIVACY EXCEPTIONALISM? 87
A. Limited Exceptional Models Outside of Health Care 89
B. State Privacy Law 90
C. Exceptionalism at the Federal Level 93
IV. REFORMING HEALTH PRIVACY REGULATION IN THE FACE OF BIG DATA 97

 This article is based on presentations delivered at Case Western Reserve University School of Law's Law-Medicine Center Symposium on Secondary Uses of Health Care Data, April 5, 2013 and the Health Law Teacher's Conference at Seton Hall University School of Law, June 8, 2013. I thank Professor Miriam Murphy who helped immeasurably with research and Scott R. Spicer, Indiana University Robert H. McKinney School of Law JD/MBA Candidate 2016, who assisted with timely and perceptive edits. Of course, the errors that remain are mine.

† Hall Render Professor of Law & Director of the Hall Center for Law and Health, Indiana University Robert H. McKinney School of Law. Email: npterry@iupui.edu.

1. Julie Brill, Comm'r, FTC, Keynote Address at the 23rd Computers, Freedom, and Privacy Conference: Reclaim Your Name 11-12 (June 26, 2013), *available at* http://www.ftc.gov/speeches/brill/130626computersfreedom.pdf.

A. Will Big Data Join the Instrumentalist Narrative? *99*
B. The Unlikely Alternative of Self-Regulation..... *101*
C. The Case for a New Upstream Data Protection Model..... *103*
CONCLUSION 106

INTRODUCTION

Health data protection in this country has exhibited two key characteristics: a dependence on downstream data protection models and a history of health privacy exceptionalism. Regarding the former, while upstream data protection models limit data collection, downstream models primarily limit data distribution *after* collection. Regarding the latter, health care privacy exhibits classic exceptionalism properties. Traditionally and for good reason health care is subject to an enhanced sector-based approach to privacy regulation.[2]

The article argues that, while "small data" rules displaying these two characteristics protect conventional health care data (doing so exceptionally, if not exceptionally well), big data facilitates the creation of health data proxies that are relatively unprotected. As a result, the carefully constructed, appropriate and necessary model of health data privacy will be eroded. Proxy data created outside the traditional space protected by extant health privacy models threatens to deprecate exceptionalism, reducing data protection to the very low levels applied to most other types of data. The rise of data proxies leads also to the questioning of our established downstream data protection model as the favored regulatory model.

This article proceeds as follows: In Part I the traditional health privacy regimes (such as HIPAA)[3] that protect "small" data are

2. *See generally* Nicolas P. Terry, *Protecting Patient Privacy in the Age of Big Data*, 81 UMKC L. REV. 385 (2012) [hereinafter Terry, *Protecting Patient Privacy*].

3. "HIPAA" as used herein refers to the HIPAA Privacy and Security rules promulgated under the Health Insurance Portability and Accountability Act of 1996. 45 C.F.R. § 164 (2013). The Privacy Rule was published in December 2000 but modified in August 2002. *Compare* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,462 (Dec. 28, 2000) *with* Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,182, 53, 182 (Aug. 14, 2002). Under the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act), the Secretary was given additional rule-making powers. *See generally* Pub. L. No. 111-5, 123 Stat. 226 (2009). Many of the modifications to HIPAA privacy and security rules were contained in the so-called Omnibus Rule. *See* Modifications to the HIPAA Privacy, Security, Enforcement, and

explained, as is the growing robustness of downstream data protection models in traditional health care space, including federal breach notification. Part II examines big data and its relationship with health care, including the data pools in play, and pays particular attention to three sources of data used to populate health proxies: "laundered" HIPAA data, patient-curated data, and medically-inflected data. Part III reexamines health privacy exceptionalism across legislative and regulatory domains seeking to understand its level of "stickiness" when faced with big data. Part IV examines how health privacy exceptionalism maps to the currently accepted rationales for health privacy and discusses the relative strengths of upstream and downstream data models in curbing what is viewed as big data's serious assault on health privacy.

I. HEALTH PRIVACY AND "SMALL" DATA

The HIPAA-HITECH data protection model dominates U.S. health privacy regulation. Since its unveiling in 1999, HIPAA's idiosyncratic regulatory model has established itself as one of the most disliked (by health care providers) and critiqued (even by privacy advocates) pieces of regulation in the history of health care.

Over the years HIPAA has faced criticism for the narrowness of its reach (e.g., health insurers but not life insurers, health care providers but not employers, awkwardly captured business associates, etc.), the expansive nature of its exceptions and authorizations, and poor enforcement.[4] In light of its flaws, as HIPAA enters its teenage years it is appropriate to reflect on its considerable maturation.

A. Understanding the HIPAA Model

Unlike the regulations that operationalize it, the HIPAA model of health care privacy protection is relatively uncomplicated, if conceptually flawed. Federal interest in protected health information[5] originated as part of HIPAA's "Administrative Simplification" model that was designed to maximize the electronic exchange flow of health care information involved in financial and administrative transactions.[6] Almost two decades later the Affordable Care Act (ACA) has

Breach Notification Rules and Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5566 (Jan. 25, 2013) (codified at 45 C.F.R. pts. 160, 164).

4. *See generally* Nicolas P. Terry, *What's Wrong with Health Privacy?*, 5 J. HEALTH & BIOMED. L. 1 (2009); Nicolas P. Terry & Leslie P. Francis, *Ensuring the Privacy and Confidentiality of Electronic Health Records*, 2007 U. ILL. L. REV. 681, 683-84 (2007).

5. 45 C.F.R. § 160.103 (2012).

6. 45 C.F.R. pt. 162 (2012). *See generally HIPAA Administrative Simplification Statute and Rules*, U.S. DEP'T OF HEALTH & HUMAN

further addressed this aspiration.[7] Additionally, the HIPAA data protection model is based on the highly instrumental view that patient health (and frequently other, more *public* health goals) are maximized by collecting and storing *all* patient information and allowing it to flow freely within a health care entity.

So understood, the HIPAA model displays some logically consistent tenets. First, the HIPAA Privacy Rule employs a downstream data protection model ("confidentiality") that seeks to contain the collected data within the health care system by prohibiting its migration to non-health care parties.[8] Second, because the data protection model is a downstream one, it does not in any way impede the collection of patient data (as would a true upstream, collection-focused "privacy" model).

Third, the HIPAA Security Rule, another downstream model, imposes physical and technological constraints on patient data storage designed to make it difficult for those outside of the health care system to acquire such data without consent. Indeed, recently, and further discussed below,[9] HITECH has introduced a further downstream model, breach notification, which requires those inside the health care system to disclose data breaches that expose patient information to outsiders. Finally, the HIPAA architects took the view that health care entities were not alone in requiring relatively unfettered access to patient data. Health care entities that outsource tasks (such as legal or IT services) would need to give their contractors (known as "Business Associates") access, and some public entities (such as the legal system and public health authorities) frequently required some level of access.

These HIPAA fundamentals help explain, if not justify, some of the flaws of its data protection model. First, comprehensive information about a patient seems to flow too easily within a health care entity. That flow is only minimally constrained by the "minimum necessary" standard applicable to "payment" and "healthcare operations"[10] but not at all when used for treatment purposes when, say, restricting access to the treatment team might have been a better option.[11]

SERVS., http://www.hhs.gov/ocr/privacy/hipaa/administrative/index.html (last visited Jan. 19, 2014).

7. *See* Patient Protection and Affordable Care Act of 2010, Pub. L. No. 111-148, § 1104, 124 Stat. 146 (2010).

8. *See, e.g.*, 45 C.F.R. § 164.502 (2012).

9. *See infra* Part I.C.

10. 45 C.F.R. §§ 164.502(b), 164.514(d) (2013).

11. *See, e.g.*, Terry & Francis, *supra* note 4, at 731-33.

Second, although we can assume (perhaps generously) that the health care entity originally collected the patient data solely for treatment and billing purposes (sometimes called *primary* use), HIPAA contains few meaningful constraints on subsequent (or *secondary*) uses of this data. The litany of such potential uses includes health quality measurement, reporting, improvement, patient safety research, clinical research, commercial uses including marketing and even the sale of patient data. Stakeholders tend to disagree on where to draw the line as to the appropriate use of patient data, and HIPAA, at least prior to HITECH, included little guidance.[12]

Third, and of considerable importance to the arguments advanced in this article, HIPAA does not literally protect data. That is, the data subject's privacy rights do not attach to and flow with the data. HIPAA, like the common law rules that preceded it,[13] created a liability rather than a property model.[14] Unlike those common law rules (such as the breach of confidence), HIPAA provides that the liability rule's remedy inures to the benefit of the regulator rather than the data-subject. The font of this liability model, imposing a duty of confidentiality on the covered entity-patient relationship,[15] *is* broader than the now obsolete bilateral physician-patient relationship, yet still attaches (and limits) data protection to traditional health care relationships and environments. In a statement predating the HIPAA statute the Institute of Medicine argued for the contrary, "[L]egislation should clearly establish that the confidentiality of person-identifiable data is an attribute afforded to the data elements themselves, regardless of who holds the data."[16] The fact that federal legislators and regulators ignored this exhortation has led to a situation whereby data-brokers can collect, process, and distribute health data outside of regulated space.

12. *See generally* NAT'L COMM. ON VITAL AND HEALTH STATISTICS, ENHANCED PROTECTIONS FOR USES OF HEALTH DATA: A STEWARDSHIP FRAMEWORK FOR "SECONDARY USES" OF ELECTRONICALLY COLLECTED AND TRANSMITTED HEALTH DATA (2007), *available at* http://www.ncvhs.hhs.gov/071221lt.pdf.

13. *See generally* Alan B. Vickery, Note, *Breach of Confidence: An Emerging Tort*, 82 COLUM. L. REV. 1426, 1428 (1982).

14. *See generally* Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089 (1972).

15. *See, e.g.*, 45 C.F.R. § 164.502(a) (2012).

16. INST. OF MED., HEALTH DATA IN THE INFORMATION AGE: USE, DISCLOSURE, AND PRIVACY 191 (Molla S. Donaldson & Kathleen N. Lohr, eds., 1994).

B. The Maturation of HIPAA

As should already be obvious it is relatively easy to pick holes in the HIPAA privacy model. The litany of its flaws has always been sizeable. And although passing years have never seen any serious attempt to address its fundamental flaws (e.g., its narrow applicability to traditional health care "covered entities"), persistent regulatory tinkering has brought about a far more robust confidentiality and security model.

In 2009 the still youthful HIPAA clearly benefited mightily from the HITECH Act,[17] although it must be acknowledged that the change in administrations with which the Act coincided likely was as important as the substantive tweaking to the regulatory model. While HITECH failed to address one cluster of HIPAA criticisms (the uncontrolled flow of patient information within health care entities), it did tackle some of the secondary uses by tightening up the consent processes for the use of patient data for marketing and the sale of patient data.[18] And although HITECH also failed to address the leakage of HIPAA-protected data through entities such as public health departments,[19]it reconfigured the legal relationship of Business Associates (BA). Although BA agreements are still required, BAs themselves are now directly subject to the Privacy Rule and, more importantly, to its enforcement and penalties.[20]

Most noticeable, however, has been the fundamental shift in enforcement. HIPAA privacy and security introduced a potentially robust process model of compliance, enforcement, and penalties. HITECH modified the penalty framework,[21] and the Obama Administration responded by coordinating all enforcement under the Office of Civil Rights (OCR)[22] and appointing a career prosecutor to head its efforts.[23] Soon thereafter OCR was investigating major privacy and

17. The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, was signed into law on February 17, 2009. HITECH Act, Pub. L. No. 111-5, 123 Stat. 227 (2009) (codified at scattered parts of 42 U.S.C.).

18. *See* HITECH Act § 13405.

19. See *infra* note 85 and accompanying text.

20. *See* HITECH Act §§ 13401, 13408.

21. HITECH Act § 13410.

22. *See Office for Civil Rights*, U.S. DEP'T. OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/office/index.html (last visited Jan. 11, 2014).

23. *See Office for Civil Rights Director Leon Rodriguez*, U.S. DEP'T. OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/office/biographydirectorrodriguez.html (last visited Jan. 11, 2014).

security breach cases and levying "statement" penalties.[24] HITECH's breach notification model, discussed below, seems to have had an impact here as data custodians and their BAs have to report when patient data has been compromised.

While increasingly incremental in nature, further tweaks to HIPAA's "small data" regulatory model are likely. The "minimum necessary" standard may be revisited and data segmentation models may slow the movement of entire patient files within institutions.[25] But overall, while still overly cumbersome and lacking clear, generalized principles, today's HIPAA has emerged as a relatively strong downstream protection model with active and effective enforcement.

C. The Omnibus Rule and Breach Notification

Because HIPAA health privacy exceptionalism has been tied to downstream protection models, it was not surprising that the increased privacy protection (and exceptionalism) introduced by HITECH saw a doubling down on downstream protection with breach notification, a rule now fleshed out by the 2013 omnibus privacy rule.[26]

With a legislative requirement to notify a data subject of a data breach, the data custodian's duty is triggered upon loss of control of the data, making a breach notification rule the definitive downstream protective model. Breach notification laws proliferated because of the dramatic increase in identity theft.[27] Although all federal agencies are

24. *See Health Information Privacy Enforcement Highlights*, U.S. DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/enforcement/highlights/index.html (last visited Jan. 11, 2014).

25. *See generally* Mark A. Rothstein, *Access to Sensitive Information in Segmented Electronic Health Records*, 40 J.L. MED. & ETHICS 394, 396 (2012).

26. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5556, 5556 (Jan. 25, 2013) (codified at 45 C.F.R. pts. 160, 164).

27. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-02-363, IDENTITY THEFT, PREVALENCE AND COST APPEAR TO BE GROWING (2002), *available at* http://www.gao.gov/assets/240/233900.pdf; LYNN LANGSTON, U.S. DEP'T OF JUSTICE, IDENTITY THEFT REPORTED BY HOUSEHOLDS, 2005-2010 (2011), *available at* http://www.bjs.gov/content/pub/pdf/itrh0510.pdf; *see also* Neil Versel, *Cyber Crooks Target Healthcare For Financial Data*, INFO. WEEK, (Oct. 24, 2012), http://www.informationweek.com/healthcare/security-privacy/cyber-crooks-target-healthcare-for-finan/240009668. *See generally* Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 HASTINGS L.J. 1227 (2003); Lynn M. LoPucki,

subject to a robust breach notification policy,[28] federal legislation to cover private parties has been proposed but not yet passed.[29] In contrast, and in the decade following California's 2002 example,[30] forty-six states and the District of Columbia have enacted breach notification laws.[31]

More recently attention has turned to medical identity theft.[32] It has been argued that medical identities are highly valued by criminals because of the comprehensive data that are contained in, for example, a stolen electronic medical record (EMR).[33] A 2006 report from The World Privacy Forum focused attention on the issue,[34] and in 2009 the Office of the National Coordinator for Health Information Technology (ONC) commissioned a study on the subject from Booz Allen Hamilton.[35] Today both the Department of Health and Human

Human Identification Theory and the Identity Theft Problem, 80 TEX. L. REV. 89 (2001).

28. *See* Memorandum from Clay Johnson III, Deputy Dir. for Mgmt., Office of Mgmt. and Budget, to the Heads of Exec. Dep'ts and Agencies (May 22, 2007), *available at* http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf.

29. *See* GINA STEVENS, CONG. RESEARCH SERV., R42475, DATA SECURITY BREACH NOTIFICATION LAWS (2012), *available at* http://www.fas.org/sgp/crs/misc/R42475.pdf (detailing the failed federal bills).

30. S.B. 1386, 2002 Leg., Reg. Sess. (Cal. 2003) (amending Cal. Civ. Code §§ 1798.29, 1798.82, and 1798.84 and itself amended by S.B. 24, 2010 Leg., Reg. Sess. (Cal. 2011)).

31. *See* STEVENS, *supra* note 29, at 4.

32. *See generally* Katherine M. Sullivan, *But Doctor, I Still Have Both Feet! Remedial Problems Faced by Victims of Medical Identity Theft*, 35 AM. J.L. & MED. 647 (2009).

33. *See generally* HEALTH RESEARCH INST., OLD DATA LEARNS NEW TRICKS: MANAGING PATIENT SECURITY AND PRIVACY ON A NEW DATA-SHARING PLAYGROUND (2011), *available at* http://pwchealth.com/cgi-local/hregister.cgi/reg/old-data-learns-new-tricks.pdf.

34. WORLD PRIVACY FORUM, MEDICAL IDENTITY THEFT: THE INFORMATION CRIME THAT CAN KILL YOU (2006), *available at* http://www.worldprivacyforum.org/wp-content/uploads/2007/11/wpf_medicalidtheft2006.pdf.

35. U.S. DEP'T OF HEALTH AND HUMAN SERVS., OFFICE OF THE NAT'L COORDINATOR FOR HEALTH INFO. TECH., MEDICAL IDENTITY THEFT FINAL REPORT (2009), *available at* http://www.healthit.gov/sites/default/files/medidtheftreport011509_0.pdf.

Services (HHS)'s Office of Inspector General[36] and the Federal Trade Commission (FTC)[37] web sites have information pages concerning medical identity theft. According to a 2012 Ponemon Institute study, 52% of health care organizations experienced one or more incidents of medical identity theft.[38] The *2013 Survey on Medical Identity Theft* (also conducted by the Ponemon Institute) estimated a 19% increase in medical identity theft victims year-to-year.[39]

Relatively few states include health data within their definition of the personal information subject to breach notification.[40] Others, true to the U.S. sector-based approach to privacy regulation, *exclude* data covered by, say, HIPAA or the Gramm-Leach-Bliley Act of 1999 (GLBA).[41]

HITECH introduced two closely related breach notification regimes. The first, introduced by Section 13402, requires HIPAA covered entities[42] and HIPAA BAs[43] to provide notification following a breach of "unsecured protected health information."[44] The second, courtesy of Section 13407, imposes a similar duty on vendors of personal health records (PHR)[45] and their third party service providers[46] with regard to "Unsecured PHR Identifiable Health Information."[47] Rulemaking authority and enforcement are vested in the HHS regarding the former and the FTC regarding the latter.[48]

---

36. *Medical ID Theft/Fraud Information*, OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HEALTH & HUMAN SERVS, http://oig.hhs.gov/fraud/medical-id-theft/index.asp (last visited Jan. 19, 2014).

37. *Id.*

38. PONEMON INST., THIRD ANNUAL BENCHMARK STUDY ON PATIENT PRIVACY & DATA SECURITY 13 (2012), *available at* http://www2.idexpertscorp.com/assets/uploads/ponemon2012/Third_Annual_Study_on_Patient_Privacy_FINAL.pdf.

39. PONEMON INST., 2013 SURVEY ON MEDICAL IDENTITY THEFT 5 (2013).

40. *See* STEVENS, *supra* note 29, at 6.

41. *Id.*

42. *See* HITECH Act, Pub. L. No. 111-5, § 13402(a), 123 Stat. 260 (2009).

43. § 13402(b).

44. § 13402(h)(1)(A) ("[P]rotected health information that is not secured through the use of a technology or methodology specified by the Secretary.").

45. § 13407(a).

46. § 13407(b).

47. § 13407(f)(3).

48. § 13407(g)(1). *See generally, Health Privacy,* FTC, http://business.ftc.gov/privacy-and-security/health-privacy (last visited Jan. 11, 2014).

The regulation of PHRs is a limited (but ultimately unsuccessful) attempt to expand health data protection from a narrow sector-provider based model (e.g., information held by a covered entity) to a data-type based model. Unfortunately it stopped short of a broad data-type model (e.g., by protecting the data itself held by *any* data custodian), limiting the custodian cohort to PHR providers.[49]

It is an interesting question why HITECH added a breach notification data protection model. Certainly medical identity theft was being raised as an issue.[50] As likely this rethinking of the approach to data protection may have been triggered by the expansion of personal health records services offered by non-health companies such as Google.[51] Maybe the HITECH architects could not agree on a way to open up the broader and established HIPAA model to apply to non-traditional custodians of health data (BAs aside) and so had to settle on a new but limited data protection model as the legislative alternative. Notwithstanding, the result was that HITECH authorized regulatory activity by the FTC that would mirror the work of HHS in the more narrowly defined, traditional health space. Ironically, however, by the time HITECH was passed the PHR business was slowing and Google Health, the PHR poster-child, soon would be closed.[52]

Following their HITECH mandate both HHS and FTC issued broadly similar interim breach notification regulations.[53] For example, the rules provided for safe harbors identifying technological standards (such as encryption levels) that negated the notification duty even if the data was acquired by a third party. The HHS rule provided that a notifiable "breach" occurred when the security or privacy of the protected health information was compromised because it posed "a significant risk of financial, reputational or other harm to the individual."[54] Such a breach triggered a responsibility to notify affected

49. *See infra* note 98.

50. *See* WORLD PRIVACY FORUM, *supra* note 34; U.S. DEP'T OF HEALTH & HUMAN SERVS., *supra* note 35.

51. *See generally* Steve Lohr, *Dr. Google and Dr. Microsoft,* N.Y. TIMES (Aug. 13, 2007), http://www.nytimes.com/2007/08/14/technology/14iht14healthnet.7107507.html?pagewanted=all.

52. For further reflections on the demise of Google Health, see Nicolas Terry, *Information Technology's Failure to Disrupt Healthcare*, 13 NEVADA L.J. 722, 745-49 (2013).

53. Breach Notification for Unsecured Protected Health Information, 74 Fed. Reg. 42,740 (Aug. 24, 2009) (to be codified at 45 C.F.R. pts. 160, 164); Breach Notification for Unsecured Protected Health Information, 74 Fed. Reg. 42,962 (August 24, 2009) (to be codified 16 C.F.R. pt. 318).

54. 45 C.F.R. § 164.402 (2009).

individuals,[55] the media,[56] and the Secretary.[57] In cases of breaches involving 500 or more individuals, immediate notification to the Secretary is required[58] in order to enable posting on the "Wall of Shame" as provided for by HITECH.[59]

In 2013 HHS published the so-called Omnibus Rule, a final rule in large part rolling up several previously published interim rules that had been authorized by HITECH.[60] The Omnibus Rule's definition of breach is substantially different from that in the interim rule. First, "an [unpermitted] acquisition, access, use or disclosure of protected health information" now is presumed to be a breach.[61] Second, the covered entity carries the burden of refuting that presumption with a risk assessment that considers:

> (i) the nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
> (ii) the unauthorized person who used the protected health information or to whom the disclosure was made;
> (iii) whether the protected health information was actually acquired or viewed; and
> (iv) the extent to which the risk to the protected health information has been mitigated.[62]

In contrast, the FTC rule applicable to non-HIPAA PHR vendors relies on the somewhat "older" approach to breach whereby "[u]nauthorized acquisition will be presumed to include unauthorized access to unsecured PHR identifiable health information" absent "reliable evidence showing that there has not been, or could not reasonably have been, unauthorized acquisition of such information."[63] Not only do somewhat different rules apply to breach notification regarding essentially similar EMR or PHR data, but security breaches

55. § 164.404.

56. § 164.406.

57. § 164.408(a).

58. § 164.408(b).

59. *See* HITECH Act, Pub. L. No. 111-5, § 13402(e)(4), 123 Stat. 262 (2009).

60. *See* Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules and Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5566 (Jan. 25, 2013) (to be codified at 45 C.F.R. pts. 160, 164).

61. 45 C.F.R. § 164.402 (2013).

62. *Id.*

63. Health Breach Notification Rule, 16 C.F.R. pt. 318 (2009).

regarding health data in the hands of custodians who are neither HIPAA entities nor PHR vendors generally do not require breach notification. Specifically, this regulatory gap works in favor of big data custodians of non-HIPAA (medically inflected) health data or "laundered" HIPAA data. A sufficiently serious breach in the face of poor security practices or technology might trigger an FTC inquiry.[64] Such eventuality aside, the only possible regulatory model would be state law breach notification. As already noted, few state laws include health information within their definitions of protected data,[65] though there are exceptions such as the California law.[66]

Breach notification as a data protection model is deserving of some criticism. It is only triggered when, necessarily, data protection has failed,[67] and it is a somewhat immature data protection model that likely will need additional calibration as we analyze its under-regulation or over-regulation tendencies. For example, to the extent that more experience tells us that we may be over-regulating some types of minor breaches it might be sensible to allow for an apology-plus-purchase of insurance defense or safe harbor.

Notwithstanding, HITECH's version seems to have some value. First, as clearly intended by the statute,[68] the "Wall of Shame" website acts as a strong deterrence system.[69] As more data is collected about the porousness of our health care providers' systems, a simple web listing could evolve into a more robust and useful ranking model across privacy and security dimensions, as (for example) with the quality/safety-based *Hospital Compare*.[70] Second, the notification system has become an important part of OCR enforcement as the agency relies on breach notifications to initiate privacy and security rule enforcement.[71]

---

64. *See infra* note 180 and accompanying text.

65. *See* STEVENS, *supra* note 29, at 6.

66. CAL. CIV. CODE ANN. §§ 1798.29(g)(4), (5) (2012). *See also* CAL. HEALTH & SAFETY CODE § 1280.15(b) (2012).

67. *See, e.g.*, Nicolas P. Terry, *Personal Health Records: Directing More Costs and Risks to Consumers?*, 1 DREXEL L. REV. 216, 245 (2009).

68. *See* HITECH Act, Pub. L. No. 111-5, § 13402(e)(4), 123 Stat. 262 (2009).

69. *See Health Information Privacy Breaches Affecting 500 or More Individuals*, U.S. DEP'T OF HEALTH & HUMAN SERVS., *available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html (last visited Jan. 11, 2014).

70. *See generally Hospital Compare*, MEDICARE.GOV, http://www.medicare.gov/hospitalcompare/ (last visited Jan. 11, 2014).

71. For example, a May 2013 settlement with Idaho State University for Security Rule violations followed receipt of a notification of breach to HHS. U.S. Dep't of Health and Hum. Servs. v. Idaho St. Univ. (May 10,

On balance, breach notification has strengthened its fellow downstream protection models – HIPAA confidentiality and security. First, the HITECH Act's breach notification model includes a public "shaming" deterrent designed to improve compliance with the HIPAA rules.[72] Second, and obviously, notifying HHS of a substantial breach invites investigation by OCR.

Overall (and likely this was an unintended consequence) breach notification is an endorsement of health privacy exceptionalism with its regulatory model applying to very narrow slices of health data custodians (HIPAA, PHR and "others"). However, the narrowness of its definition and its quintessential downstream data protection model confirm its irrelevance in any search for a federal privacy response to big data's growing hold on medically inflected data.

II. THE DATA PROXIES' CHALLENGE TO HEALTH PRIVACY

Big data is so named because of its unprecedented volume and for its "complexity, diversity, and timeliness."[73] Big data refers not only to the collection and storage of extremely large data sets but also the data mining and predictive analytic routines that process the data, the latter being understood as "[t]echnology that learns from experience (data) to predict the future behavior of individuals in order to drive better decisions."[74]

Essentially big data is the latest type of business intelligence (BI), or, to frame it slightly differently, the latest BI analytics are what

---

2013) (resolution agreement), *available at* http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/isu-agreement.pdf. Similarly, a July 2013 resolution agreement with the managed care provider WellPoint, Inc., called for a payment of $1.7m after the exposure of 612,402 records. U.S. Dep't of Health and Hum. Servs. v. WellPoint, Inc. (July 8, 2013) (resolution agreement), *available at* http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/wellpoint-agreement.pdf.

72. HITECH Act § 13402(e)(4) ("The Secretary shall make available to the public on the Internet website of the Department of Health and Human Services a list that identifies each covered entity involved in a breach … in which the unsecured protected health information of more than 500 individuals is acquired or disclosed.").

73. PETER GROVES ET AL., CTR. FOR U.S. HEALTH SYS. REFORM, BUS. TECH. OFFICE, THE "BIG DATA" REVOLUTION IN HEALTHCARE: ACCELERATING VALUE AND INNOVATION 1 (2013), *available at* http://www.mckinsey.com/insights/health_systems_and_services/~/media/mckinsey/dotcom/insights/health%20care/the%20big-data%20revolution%20in%20us%20health%20care/the_big_data_revolution_in_healthcare.ashx.

74. ERIC SIEGEL, PREDICTIVE ANALYTICS: THE POWER TO PREDICT WHO WILL CLICK, BUY, LIE, OR DIE 11 (2013).

extract value from big data.[75] Not surprisingly, MBA-speak business jargon dominates the space. Thus, according to Gartner, Inc., "'Big data' is high-volume, –velocity and –variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making."[76] It is important not to underestimate one of these three properties: high-variety. Big data does not use structured databases (or at least is not as reliant on them as previous generation systems such as credit reporting) but *is* capable of absorbing high-variety data. Data sources (or data pools) continually change and expand; yet big data seems adept at digesting them. As described in a recent report by the Centre For Information Policy Leadership:

> While traditionally analytics has been used to find answers to predetermined questions, its application to big data enables exploration of information to see what knowledge may be derived from it, and to identify connections and relationships that are unexpected or were previously unknowable. When organisations employ analytics to explore data's potential for one use, other possible uses that may not have been previously considered often are revealed. Big data's potential to yield unanticipated insights, the dramatically low cost of information storage and the rapidly advancing power of algorithms have shifted organisations' priorities to collecting and harnessing as much data as possible and then attempting to make sense of it.[77]

The analytics of big data seek to predict the behavior not only of populations or cohorts but also of individuals. In *Predictive Analytics:*

75. *See generally* Doron Aspitz, *It's Time to Instill More BI Into Business Intelligence*, WIRED (May 6, 2013), http://www.wired.com/insights/2013/05/its-time-to-instill-more-bi-into-business-intelligence. *See also* Tom Pringle, *Putting the Business Back into Business Intelligence*, INFO. AGE (July 4, 2013), http://www.information-age.com/technology/information-management/123457179/putting-the-business-back-into-business-intelligence.

76. Svetlana Sicular, *Gartner's Big Data Definition Consists of Three Parts, Not to Be Confused with Three "V"s*, FORBES (Mar. 27, 2013), http://www.forbes.com/sites/gartnergroup/2013/03/27/gartners-big-data-definition-consists-of-three-parts-not-to-be-confused-with-three-vs. *See also* Andrew McAfee & Erik Brynjolfsson, *Big Data: The Management Revolution*, HARV. BUS. REV., Oct. 2012, at 62.

77. CTR. FOR INFO. POL'Y LEADERSHIP, BIG DATA AND ANALYTICS: SEEKING FOUNDATIONS FOR EFFECTIVE PRIVACY GUIDANCE, A DISCUSSION DOCUMENT 1 (2013), *available at* http://www.hunton.com/files/Uploads/Documents/News_files/Big_Data_and_Analytics_February_2013.pdf.

The Power to Predict Who Will Click, Buy, Lie, or Die, computer scientist Eric Siegel explained the distinction as follows:

> Forecasting makes aggregate predictions on a macroscopic level. How will the economy fare? Which presidential candidate will win more votes in Ohio? Whereas forecasting estimates the total number of ice cream cones to be purchased next month in Nebraska, predictive technology tells you which *individual* Nebraskans are most likely to be seen with cone in hand.[78]

In the context of health information the business intelligence grail is to identify and exploit a patient's differential health status. According to Neil Biehn, with such segmentation "organizations can more easily identify anomalous buying behavior and make intelligent product and offer recommendations that are statistically more likely to be purchased."[79] Biehn continues, "If two customers are alike but not buying the same products, the data analysis can advise which opportunities the sales team might be missing," concluding that "[t]his is the type of Big Data viability that moves the needle in the real world."[80]

The privacy implications of individuated big data analysis are profound. Beyond the expropriation or "using" objections to such data collection and processing, such as Commissioner Brill's critique quoted at the beginning of this article,[81] the computer modeling of predictive analytics predicts a world of dehumanizing "data determinism." FTC Chairwoman Edith Ramirez described "data determinism" as the judgment of persons:

> . . . not because of what they've done, or what they will do in the future, but because inferences or correlations drawn by algorithms suggest they may behave in ways that make them poor credit or insurance risks, unsuitable candidates for employment or admission to schools or other institutions, or unlikely to carry out certain functions.[82]

78. SIEGEL, *supra* note 74, at 12.

79. Neil Biehn, *Realizing Big Data Benefits: The Intersection of Science and Customer Segmentation*, WIRED (June 7, 2013, 11:32 AM), http://insights.wired.com/profiles/blogs/realizing-big-data-benefits-the-intersection-of-science-and.

80. *Id.*

81. *See supra* note 1 and accompanying text.

82. Edith Ramirez, Chairwoman, FTC, Keynote Address at the Tech. Pol'y Inst. Aspen Forum: The Privacy Challenges of Big Data: A View From the Lifeguard's Chair 7 (Aug. 19, 2013), *available at* http://ftc.gov/speeches/ramirez/130819bigdataaspen.pdf.

Finally, there is the "Doomsday" scenario – a big data breach. The industrial scale data-warehousing model is the antithesis of the "silo" model of data storage used in the pre-information age. The lack of data liquidity (with all of its informational disadvantages) inherent in that model meant that there was little profit or harm in an isolated security breach. The opposite is true with big data storage. However, there are reports that big data brokers are not immune from the same security breaches that are plaguing other businesses.[83]

A. "Laundered" HIPAA Data

One key to appreciating this threat to health privacy is to understand the health care data pools that big data seeks to leverage. In *The "Big Data" Revolution in Healthcare*, the McKinsey Global Institute identifies four primary data pools "at the heart of the big-data revolution in healthcare": activity (claims) and cost data, clinical data, pharmaceutical R&D data, and patient behavior and sentiment data.[84] Previously I have argued that proprietary concerns will likely slow the sharing of drug and device data by manufacturers or claims and related financial data by health care providers while hurdles to interoperability will hinder the migration of clinical data from EMRs.[85] More immediately big data is using three types of health-specific data to construct proxies for HIPAA-protected data. These are "laundered" HIPAA data, patient-curated information, and medically inflected (e.g. patient behavior and sentiment) data.

There has always been something lopsided about the HIPAA regulatory model. Rather than concentrating on securing health data, most of the Privacy Rule provisions detail wide-ranging exceptions (public health, judicial, and regulatory) to data protection or outline the *process* by which patients can consent to disclosure.[86] Just recently, for example, a pharmacy chain made the headlines by conditioning its loyalty rewards program on a broad HIPAA authorization.[87] It is no surprise, therefore, to learn that there has been leakage of health data through the very system set up to protect it. Such leakage has been exacerbated by the mission creep exhibited by

83. Brian Krebs, *Data Broker Giants Hacked by ID Theft Service*, KREBSONSECURITY (Sept. 13, 2013), http://krebsonsecurity.com/2013/09/data-broker-giants-hacked-by-id-theft-service/.

84. GROVES ET AL., *supra* note 73, at 4.

85. Terry, *Protecting Patient Privacy*, *supra* note 2, at 392.

86. Terry & Francis, *supra* note 4, at 714-15.

87. David Lazarus, *CVS Thinks $50 is Enough Reward for Giving Up Healthcare Privacy*, L.A. TIMES (Aug. 15, 2013), http://www.latimes.com/business/la-fi-lazarus-20130816,0,2932825.column.

the recipients of data under HIPAA, particularly public health agencies. As Wendy Mariner notes:

> Today, almost everyone, regardless of station, could be subject to public health surveillance. The scope of public health surveillance has grown significantly beyond its contagious disease origins . . . . [A] new generation of reporting laws reflects a goal of many people in public health: to collect data about chronic diseases outside the context of a research study and without the need to obtain any individual patient's informed consent. . . . Do they offer the promise of medical advances, or the threat of "general searches, which the authors of the Bill of Rights were so concerned to protect against?"[88]

For example, a 2013 report from the Citizens' Council for Health Freedom alleges broad state health surveillance based on individual and often identifiable records.[89] However, public health authorities are not only voraciously consuming patient data but also abetting the acquisition of the same by big data companies.

Researchers at Harvard's Data Privacy Lab have found that thirty-three states *re*-release patient hospital discharge data that they have acquired as HIPAA-permitted recipients of patient data.[90] Generally states release this data (that is no longer in the HIPAA-protected zone) in somewhat de-identified or anonymized form but with little restriction on future use of the data. The naïve thought that such data was only being released to academic researchers was upended by the Data Privacy Lab's discovery that many of the major buyers of such state health databases were big data companies.[91] Most states only charge small fees that are not a major source of revenue for them, and many are oblivious to this practice.[92]

---

88. Wendy K. Mariner, *Mission Creep: Public Health Surveillance and Medical Privacy*, 87 B.U. L. REV. 347, 350-51 (2007) (quoting TECH. & PRIV. ADVISORY COMM., U.S. DEP'T OF DEFENSE, SAFEGUARDING PRIVACY IN THE FIGHT AGAINST TERRORISM 48-49 (2004), *available at* http://www.cdt.org/security/usapatriot/20040300tapac.pdf).

89. Press Release, Citizens' Council for Health Freedom, 50-State Report Unveiled; States Track Medical Data from Birth to Death without Consent (Aug. 21, 2013), http://www.cchfreedom.org/cchf.php/802#.UheQzRukr9I.

90. SEAN HOOLEY & LATANYA SWEENEY, HARV. UNIV., DATA PRIV. LAB, SURVEY OF PUBLICLY AVAILABLE STATE HEALTH DATABASES 3 (2013), *available at* http://dataprivacylab.org/projects/50states/1075-1.pdf.

91. *See, e.g.*, *Top Buyers of Publicly Available State Health Databases*, THE DATA MAP, http://thedatamap.org/buyers.html (last visited Jan. 11, 2014).

92. Jordan Robertson, *States' Hospital Data for Sale Puts Privacy in Jeopardy*, BUS. WK. (June 5, 2013),

The obvious solution is for the state public health agencies to contractually prohibit re-identification. For example, the National Practitioner Data Bank (NPDB) collects information about physician malpractice awards, adverse licensure reports, and Medicare/Medicaid exclusions.[93] Although it is not a public resource, the NPDB does release de-identified data. Following a re-identification episode[94] NPDB now contains a prohibition on re-identification, specifically against using its "dataset alone or in combination with other data to identify any individual or entity or otherwise link information from this file with information in another dataset in a manner that includes the identity of an individual or entity."[95]

Clearly, state health departments and any similarly placed recipients of HIPAA data should require similar restrictions. Indeed, the proposed FTC privacy framework would mandate such:

> . . . [I]f a company makes such de-identified data available to other companies – whether service providers or other third parties – it should contractually prohibit such entities from attempting to re-identify the data. The company that transfers or otherwise makes the data available should exercise reasonable oversight to monitor compliance with these contractual provisions and take appropriate steps to address contractual violations.[96]

Until such prohibitions are instituted, HIPAA's public health exception unpardonably will continue to facilitate the "laundering" of protected patient data as it is transferred from a data protected domain to unprotected space.

B. The Self-Quantified, Self-Curating Patient

Ironically one of the greatest threats to an individual's health privacy is . . . the individual. One of the first examples of theretofore

---

http://www.businessweek.com/news/2013-06-05/states-hospital-data-for-sale-leaves-veteran-s-privacy-at-risk.

93. As originally mandated by the Health Care Quality Improvement Act of 1986. 42 U.S.C. *§* 11131 (2013) (providing for payment of malpractice awards); § 11132 (providing for adverse license actions); § 11133 (providing for Medicare/Medicaid exclusion).

94. *See* Duff Wilson, *Withdrawal of Database on Doctors Is Protested*, N.Y. TIMES (Sept. 15, 2011), http://www.nytimes.com/2011/09/16/health/16doctor.html?_r=0.

95. *Public Use Data File*, NAT'L PRACTITIONER DATA BANK, http://www.npdb-hipdb.hrsa.gov/resources/publicData.jsp (last visited Jan. 11, 2014).

96. FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 21 (2012), *available at* http://www. ftc.gov/os/2012/03/120326privacyreport.pdf.

HIPAA-protected data migrating to HIPAA-free space was during President George W. Bush's administration at a time when the slowing of the administration's provider-curated EMR program coincided with the launching of PHR platforms by Google and Microsoft.[97] As a result the HITECH Act architects attempted to protect for the first time health data that migrated from a protected to an unprotected (or marginally protected) zone. However, they chose to do so with a swiftly outmoded, downstream breach notification model.[98]

In the interim, different (and unregulated) technologies have emerged that encourage patient rather than provider curation of health data. The most obvious example is the federal government's "Blue Button" technology[99] that allows patients to download their records to their own devices. The "Blue Button" approach to patient access and hence *control* of their health data has become a rallying cry for many (if not all)[100] patient privacy advocates[101] and has been encouraged by President Obama's administration.[102] Indeed, then ONC National Coordinator Farzad Mostashari announced a Blue Button Mash-Up challenge to build software for patients designed to combine their downloaded Blue Button information with other data sources.[103]

---

97. *See generally* Terry, *supra* note 67.

98. *See* discussion *supra* note 49 and accompanying text.

99. *See* Lygeia Ricciardi, *The Blue Button Movement: Kicking off National Health IT Week with Consumer Engagement*, U.S. DEP'T OF VETERANS AFFAIRS, http://www.va.gov/bluebutton/ (last updated Mar. 11, 2014); *Coming Soon: The Blue Button Connector*, HEALTHIT.GOV, http://www.healthit.gov/bluebutton (last visited Jan. 11, 2014).

100. *See* Leslie P. Francis, *When Patients Interact with EHRs: Problems of Privacy and Confidentiality*, 12 HOUS. J. HEALTH L. & POL'Y 171, 172 (2012).

101. *See, e.g.*, Bill Toland, *Blue Button Puts Patient in Control*, SAN ANGELO STANDARD TIMES (July 8, 2013), http://www.gosanangelo.com/news/2013/jul/08/blue-button-puts-patient-in-control; Deborah Peel, *Experts Tout Blue Button as Enabling Information Exchange Between Medical Provider and Patient,* PATIENT PRIVACY RIGHTS (June 23, 2013), http://patientprivacyrights.org/2013/06/experts-tout-blue-button-as-enabling-information-exchange-between-medical-provider-and-patient.

102. Aneesh Chopra, *Blue Button Provides Access to Downloadable Health Data,* WHITE HOUSE OFFICE OF SCI. AND TECH. POL'Y BLOG (OCT. 7, 2010), http://www.whitehouse.gov/blog/2010/10/07/blue-button-provides-access-downloadable-personal-health-data.

103. Mary Mosquera, *Mostashari Urges Blue Button-Big Data*, HEALTHCARE IT NEWS (June 7, 2012), http://www.healthcareitnews.com/news/mostashari-urges-blue-button-big-data-mashup.

At root such patient curation of health data bespeaks autonomy and is symbolic of patient ownership of the data. However, it fails to take into account one practical limitation –the canonical version of the record will remain in the provider's control – and one legal limitation – that only the provider-curated copy is protected by HIPAA-HITECH. In contrast, the patient-curated "copy" attracts little meaningful privacy protection. Well-meaning privacy advocates should think carefully before promoting this autonomy-friendly "control" model until data protection laws (not to mention patient education as to good data practices) catch up with patient curated data.

A similarly dichotomous result is likely as the medically quantified self develops. The quantified-self movement concentrates on personal collection and curation of inputs and performance.[104] Obviously, health, wellness, and medically inflected data will likely comprise a large proportion of such data.

A similar, if less formal, scenario is emerging around health and wellness apps on smartphones and connected domestic appliances such as scales and blood pressure cuffs.[105] Smartphones are crammed with sensors for location, orientation, sound, and pictures that add richness to data collection.[106] And there is ongoing and explosive growth in the medical apps space that seeks to leverage such sensors. [107]

More and more we are going to demand control of information about ourselves *and* generate medically inflected and core health data about ourselves. These processes will in most cases lead to medically inflected data that exists outside of the HIPAA-HITECH protected zone.

C. Medically Inflected Data

Arguably the greatest challenge to the current health privacy models of data protection, and hence to health privacy exceptionalism, is the proliferation of what McKinsey refers to as patient behavior and sentiment data.[108] According to ProPublica, big

104. *See* Gary Wolf, *Know Thyself: Tracking Every Facet of Life, from Sleep to Mood to Pain, 24/7/365*, WIRED MAG. (June 22, 2009), http://www.wired.com/medtech/health/magazine/17-07/lbnp_knowthyself?currentPage=all. *See generally* QUANTIFIED SELF, http://quantifiedself.com/.

105. *See* WITHINGS, http://www.withings.com/.

106. *See* Terry *supra* note 52, at 751.

107. *See generally* Nathan Cortez, *The Mobile Health Revolution?* (SMU Dedman Sch. of L. Legal Stud. Res. Paper, No. 128, June 24, 2013), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2284448.

108. GROVES ET AL., *supra* note 73, at 4.

data companies start with basic information about individuals before adding demographics, educational level, life events, credit reports, hobbies, salary information, purchase histories, and voting records.[109] As to health information:

> Data companies can capture information about your "interests" in certain health conditions based on what you buy – or what you search for online. Datalogix has lists of people classified as "allergy sufferers" and "dieters." Acxiom sells data on whether an individual has an "online search propensity" for a certain "ailment or prescription."[110]

Unlike laundered HIPAA or patient self-curated data, these medically inflected data were not created for direct wellness or medical purposes. Rather, medically inflected data are quintessential *high-variety* big data. Their sources are diverse and include web-browsing trails,[111] exhaust data from online transactions,[112] web scrapers,[113] social media interactions,[114] mobile phone usage,[115] smartphone sensors,[116] mobile health apps,[117] and both medical[118] and non-medical

109. Lois Beckett, *Everything We Know about What Data Brokers Know about You*, PROPUBLICA (Mar. 7, 2013), http://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you.

110. *Id.*

111. *See, e.g.*, Marco D. Huesch, *Privacy Threats When Seeking Online Health Information*, 173 JAMA INTERNAL MED. 1838, 1838-40 (2013).

112. *See, e.g.*, Marcus Wohlsen, *Amazon's Next Big Business Is Selling You*, WIRED (Oct. 16, 2012), http://www.wired.com/business/2012/10/amazon-next-advertising-giant; Alistair Barr & Jennifer Saba, *Analysis: Sleeping Ad Giant Amazon Finally Stirs*, REUTERS (Apr. 24, 2013), http://www.reuters.com/article/2013/04/24/us-amazon-advertising-idUSBRE93N06E20130424.

113. *See, e.g.*, Julia Angwin & Steve Stecklow, *"Scrapers" Dig Deep for Data on Web*, WALL ST. J. (Oct. 11, 2010), http://online.wsj.com/article/SB10001424052748703358504575544381288117888.html.

114. *See, e.g.*, Rebecca Greenfield, *Facebook Now Knows What You're Buying at Drug Stores*, THE ATLANTIC WIRE (Sept. 24, 2012), http://www.theatlanticwire.com/technology/2012/09/facebook-tracking-you-drug-store-now-too/57183/.

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

116. *See, e.g.*, Yves-Alexandre de Montjoye et al., *Unique in the Crowd: The Privacy Bounds of Human Mobility*, SCIENTIFIC REPORTS, Mar. 25, 2013,

networked devices.[119] Some of this data may still be unused by big data because it is "dark data" that has been left over or discarded from other processes and not yet leveraged,[120] or, in the words of Andrew McAfee and Erik Brynjolfsson, "[T]here's a huge amount of signal in the noise, simply waiting to be released."[121]

Consider just one example of a recognized big data source: social media interactions. Michal Kosinski and colleagues analyzed the Facebook "likes" of almost 60,000 volunteers. Using big data techniques the researchers were able to predict "sexual orientation, ethnicity, religious and political views, personality traits, intelligence, happiness, use of addictive substances, parental separation, age, and gender" and speculated that "given appropriate training data, it may be possible to reveal other attributes as well."[122] As hypothesized by FTC Commissioner Julie Brill:

> [W]e can easily imagine a company that could develop algorithms that will predict . . . health conditions – diabetes, cancer, mental illness – based on information about routine transactions

---

http://www.nature.com/srep/2013/130325/srep01376/pdf/srep01376.pdf.

117. *See, e.g.*, Emily Steel & April Dembosky, *Health App Users Have New Symptom to Fear*, FIN. TIMES (Sept. 1, 2013), http://www.ft.com/intl/cms/s/0/97161928-12dd-11e3-a05e-00144feabdc0.html.

118. *See, e.g.*, Amy Dockser Marcus & Christopher Weaver, *Heart Gadgets Test Privacy-Law Limits*, WALL ST. J. (Nov. 28, 2012), http://online.wsj.com/article/SB10001424052970203937004578078820874744076.html.

119. *See, e.g.*, Evgeny Morozov, *Requiem for Our Wonderfully Inefficient World,* SLATE (Apr. 26, 2013), http://www.slate.com/articles/technology/future_tense/2013/04/senor_based_dynamic_pricing_may_be_efficient_but_it_could_create_inequality.html.

120. Isaac Sacolick, *Dark Data – A Business Definition,* SOCIAL, AGILE, AND TRANSFORMATION (Apr. 10, 2013), http://blogs.starcio.com/2013/04/dark-data-business-definition.html ("Dark data is data and content that exists and is stored, but is not leveraged and analyzed for intelligence or used in forward looking decisions.").

121. McAfee & Brynjolfsson, *supra* note 76, at 63.

122. Michal Kosinski et al., *Private Traits and Attributes Are Predictable from Digital Records of Human Behavior,* 110 PROCEEDINGS OF THE NAT'L ACAD. SCI. 5802, 5805 (2013). *See also* Katie Lobosco, *Facebook Friends Could Change Your Credit Score*, CNN (Aug. 27, 2013), http://money.cnn.com/2013/08/26/technology/social/facebook-credit-score/index.html?hpt=hp_t2 (describing how "some financial lending companies have found that social connections can be a good indicator of a person's creditworthiness").

> – store purchases, web searches, and social media posts – and sells that information to marketers and others.[123]

Hyper amounts of medically inflected data processed through advanced analytics provide data custodians with a proxy for protected health information without the HIPAA-HITECH regulatory costs, negating health privacy exceptionalism. HIPAA was designed, inter alia, to limit the secondary uses of health data, a game of *Whac-A-Mole* played out in the regulated zone with different types of prohibitions, authorizations and consents, compound authorization rules and opt-in or opt-out defaults. Big data marginalizes that game. It absorbs clinical and related data pools such as "laundered" HIPAA data and unregulated medically inflected data. As a result the new privacy reality is no longer the fifteen-year-old fight to contain secondary uses of protected data but a new problem—the *primary* use of secondary data. In the words of Viktor Mayer-Schonberger and Kenneth Cukier, "Unfortunately, the [privacy] problem has been transformed. With big data, the value of information no longer resides solely in its primary purpose . . . it is now in secondary uses." [124] In short, big data can produce basically unprotected patient-level data that will serve as an effective proxy for HIPAA-protected data.

III. HOW "STICKY" IS HEALTH PRIVACY EXCEPTIONALISM?

Claims for exceptional treatment are frequently controversial. This is the case for such diverse claims as the "American Exceptionalism" lens on foreign relations,[125] the constitutionality of health care legislation,[126] HIV-AIDS policy,[127] and so on. At the risk of being reductive, however, U.S. law encourages such exceptionalism by

123. Brill, *supra* note 1, at 7.

124. VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK 153 (2013).

125. *See generally* Harold Hongju Koh, *On American Exceptionalism*, 55 STAN. L. REV. 1479 (2003).

126. *See, e.g.*, Abigail R. Moncrieff, *Understanding the Failure of Health-Care Exceptionalism in the Supreme Court's Obamacare Decision*, 142 CHEST 559, 559-60 (2012), *available at* http://journal.publications.chestnet.org/data/Journals/CHEST/24838/559.pdf (highlighting the Supreme Court's refusal to recognize special constitutional treatment for healthcare legislation).

127. *See, e.g.*, Zita Lazzarini, *What Lessons Can We Learn from the Exceptionalism Debate (Finally)?*, 29 J.L., MED. & ETHICS 149 (2001); Scott Burris, *Public Health, "AIDS Exceptionalism" and the Law*, 27 J. MARSHALL L. REV. 251 (1994).

eschewing broad principles of privacy law of general application, in contrast to, say, European law.[128]

Yet the claims for health privacy exceptionalism are well established and have exceptional provenance. The Institute of Medicine, which "asks and answers the nation's most pressing questions about health and health care,"[129] argued prior to HIPAA:

> For the most part, privacy law in this country has been formulated under the assumption that holders of information about people may generally do with it what they please, constrained only by corporate ethics and the good taste of business, societal acceptance (or outrage), occasional attention by the government, pressures of consumer activist groups, and the consequences of legal actions brought by individuals or consumer groups. This historical view may prove inappropriate or even dangerous in regard to health data.[130]

The Institute of Medicine has since repeated this position in 2001's *Crossing the Chasm*.[131] Indeed, exceptionalism seems sufficiently well established in the domain to support claims for heightened exceptional treatment for subsets of health information, such as psychiatric privacy,[132] genetic privacy,[133] and neuro-privacy.[134]

---

128. *See generally* Viktor Mayer-Schönberger, *Beyond Privacy, Beyond Rights-Toward a "Systems" Theory of Information Governance*, 98 CAL. L. REV. 1853 (2010) (arguing that the United States' rights-based approach to information privacy has largely failed and that it would benefit from exploring a European style "information-governance system"). *See also* Nicolas P. Terry, *Privacy and the Health Information Domain: Properties, Models and Unintended Results*, 10 EUR. J. HEALTH L. 223, 228-229 (2003).

129. *About the IOM*, INST. OF MED., http://www.iom.edu/About-IOM.aspx (last updated Nov. 4, 2013).

130. INST. OF MED., *supra* note 16, at 211.

131. INST. OF MED., CROSSING THE QUALITY CHASM: A NEW HEALTH SYSTEM FOR THE 21ST CENTURY 172 (2001) ("The demands of health care with regard to security and availability are both more stringent and more varied than those of other industries.").

132. *APA Generally Pleased With HIPAA Final Privacy Rule*, PSYCHIATRIC NEWS (Jan. 24, 2013), http://alert.psychiatricnews.org/2013/01/apa-generally-pleased-with-hipaa-final.html.

133. *See, e.g.*, Lawrence O. Gostin & James Hodge, Jr., *Genetic Privacy and the Law: An End to Genetics Exceptionalism*, 40 JURIMETRICS J. 21, 23 (1999) (criticizing enhanced protection for genetic information *inter alia* on public goods grounds).

134. *See, e.g.*, Stacey A. Tovino, *Functional Neuroimaging Information: A Case for Neuro Exceptionalism?*, 34 FLA. ST. U. L. REV. 415, 485 (2007).

This section examines exceptionalism outside of the health domain and then analyzes the strength or "stickiness" of health privacy exceptionalism under state and federal law.

A. Limited Exceptional Models Outside of Health Care

US law does not protect data though any generalized regulatory system nor by reference to any general principles. Rather, the system is vertical or sector-based. As such, persistent criticisms of HIPAA privacy must be put in perspective; HIPAA stands tall when compared to protections given to personal data in other sectors.

For example, GLBA governs consumer privacy in the financial sector.[135] The Act declares that financial institutions have "an affirmative and continuing obligation to respect the privacy of [their] customers and to protect the security and confidentiality of those customers' nonpublic personal information."[136] Reminiscent of HIPAA, GLBA is emphatically sector-specific and applies to narrowly defined groups of financial data custodians. Just as HIPAA does not apply to all custodians of health care data, so GLBA does not apply to all who hold consumer financial data.[137] And like HIPAA, GLBA is a downstream data protection model that erects a duty of confidentiality[138] and requires notice to consumers of an institution's privacy policies and practices.[139] Overall, however, GLBA is far less effective than HIPAA: there is administrative confusion because of the large number of federal agencies involved; penalties or other remedies are limited; and the core non-disclosure rule is subject to seldom triggered consumer opt-out.[140]

A far narrower provision, the Reagan-era Video Privacy Protection Act of 1988 (VPPA) applies a downstream data protection model to "personally identifiable rental records" of "prerecorded video cassette tapes or similar audio visual material."[141] The written consent

135. Gramm-Leach-Bliley Act, Pub. L. No. 106-102, § 501, 113 Stat. 1338, 1436 (1999). *See generally* Edward J. Janger & Paul M. Schwartz, *The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 MINN. L. REV. 1219, 1219-20 (2002).

136. 15 U.S.C. § 6801(a) (2012).

137. *See* 15 U.S.C. § 6805(a) (2012). Notwithstanding, the FTC does have some broad residual powers. *See* Privacy of Consumer Financial Information; Final Rule, 65 Fed. Reg. 33,646 (May 24, 2000) (codified at 16 C.F.R. pt. 313).

138. 15 U.S.C § 6802(a)(1) (2012) (requiring non-disclosure of "nonpublic personal information" to "nonaffiliated third parties").

139. *See* 15 U.S.C §§ 6803(a), (c) (2012).

140. Kathleen A. Hardee, *The Gramm-Leach-Bliley Act: Five Years After Implementation, Does The Emperor Wear Clothes?*, 39 CREIGHTON L. REV. 915, 921-36 (2006).

141. Pub. L. No. 100–618, 102 Stat. 3195 (1988).

to share (opt-in) provision was watered down by the Video Privacy Protection Act Amendments Act of 2012 at the behest of streaming video providers and social media services that wished to use Internet-based consent models.[142]

Outside of these narrow exceptionally treated domains where legislators were prepared to assert private spaces, privacy protection in the U.S. has been moribund. Somewhat alone, the FTC has struggled to protect consumer privacy with outdated or clumsy theories such as false or misleading representations contained in published privacy policies.[143]

B. State Privacy Law

Health privacy and HIPAA frequently are viewed as indistinguishable. However, health privacy exceptionalism is not restricted to federal law. In the decade and a half since the appearance of the HIPAA regulations, state law regarding health privacy appears to have receded into the background. After all the Bush Administration's health information technology narrative included the characterization of divergent state laws as impeding EHR implementation. [144] Furthermore, in the intervening years several states have normalized their laws with HIPAA.[145]

There *are* explicit protections of privacy in a handful of state constitutions.[146] And some state supreme courts have implied such a

142. *See also* Cable TV Privacy Act of 1984, 47 U.S.C. § 551 (2012).

143. *See, e.g.,* Complaint at 6-7, 9, Facebook, Inc., Docket No. C-4365 (Aug. 10, 2012), *available at* http://ftc.gov/os/caselist/0923184/111129facebookcmpt.pdf; Press Release, FTC, Myspace Settles FTC Charges That It Misled Millions of Users About Sharing Personal Information with Advertisers (May 8, 2012), http://ftc.gov/opa/2012/05/myspace.shtm; Press Release, FTC, FTC Charges Deceptive Privacy Practices in Google's Rollout of its Buzz Social Network (Mar. 30, 2011), http://www.ftc.gov/opa/2011/03/google.shtm.

144. *Activities of the Office of the National Coordinator for Health Information Technology: Hearing Before the Subcomm. on Tech., Innovation, and Competitiveness of the S. Comm. on Commerce, Sci., and Transp.*, 109th Cong. (2005) (statement of David J. Brailer, M.D., Ph.D., Nat'l Coordinator for Health Info. Tech., U.S. Dep't of Health & Human Servs.), *available at* http://www.hhs.gov/asl/testify/t050630a.html (describing divergent state laws as "variations in privacy and security policies that can hinder interoperability").

145. Ann Waldo, *Hawaii and Health Care: A Small State Takes a Giant Step Forward*, O'REILLY RADAR (Aug. 21, 2012), http://radar.oreilly.com/2012/08/hawaii-health-care-law-simplicity.html (discussing House Bill 1957).

146. *See* ALASKA CONST., art. I, § 22 (amended 1972); ARIZ. CONST., art. II, § 8; CAL. CONST., art. I, § 1; FLA. CONST., art. I, § 12 (amended 1982), §

right[147] that subsequently has been applied in cases involving medical information.[148] Yet there is nothing that could be described as exceptional. In contrast, a few state legislatures embraced strong, exceptional health privacy models in the pre-HIPAA years[149] that continue to escape preemption due to HIPAA's "more stringent" provision.[150]

In fact some states have asserted resilient health privacy exceptionalism. There should be little surprise that California has built on its enviable consumer protective reputation with additional substantive and enforcement provisions. The state's original *Confidentiality of Medical Information Act* dates from 1981. It is notable for possessing a broader reach than HIPAA, applying, for example, to health data custodians who are not health care providers.[151] California passed one of the first health information breach notification laws.[152] More recently the state established the Office of Health Information Integrity to "ensure the enforcement of state law mandating the confidentiality of medical information and to impose administrative fines for the unauthorized use of medical information."[153] The law requires:

> Every provider of health care shall establish and implement appropriate administrative, technical, and physical safeguards to protect the privacy of a patient's medical information. Every provider of health care shall reasonably safeguard confidential medical information from any unauthorized access or unlawful access, use, or disclosure.[154]

Perhaps more surprisingly Texas enacted similarly broad protection for health information. In sharp contrast to the narrow HIPAA conception of a "covered entity," the Texas law applies to "any person who . . . engages . . . in the practice of assembling, collecting,

23 (amended 1998); HAW. CONST., art. I, § 6, 7 (amended 1978); ILL. CONST., art. I, § 6, 12; LA. CONST. art. I, § 5; MONT. CONST. art. II, § 10; S.C. CONST. art. I, § 10; WASH. CONST. art. I, § 7.

147. Pavesich v. New Eng. Life Ins. Co., 50 S.E. 68 (Ga. 1905).

148. *See, e.g.*, King v. State, 535 S.E.2d 492, 497 (Ga. 2000). *Cf.* State v. Davis, 12 A.3d 1271, 1276-77 (N.H. 2010).

149. *E.g.*, Confidentiality of Medical Information Act, CAL. CIV. CODE §§ 56-56.07 (West 2007 & Supp. 2013). *See also* WIS. STAT. §§ 146.81-82 (2013).

150. 45 C.F.R § 160.202 (2012).

151. CAL. CIV. CODE § 56.06(a) (2012).

152. CAL. CIV. CODE ANN. §§ 1798.29(g)(4), (5) (2012).

153. CAL. HEALTH & SAFETY CODE § 130200 (2012).

154. CAL. HEALTH & SAFETY CODE § 130203(a) (2012).

analyzing, using, evaluating, storing, or transmitting protected health information."[155] Texas also requires "clear and unambiguous permission" before using health information for marketing[156] and broadly prohibits the sale of an individual's protected health information.[157]

As discussed above, HITECH (together with a change in administration) provided the enforcement focus that HIPAA had lacked.[158] However, the 2009 legislation did not alter the longstanding HIPAA position of not permitting private rights of action.[159] Of course a small number of states permit such actions under their health privacy statutes.[160] However, almost all jurisdictions allow some species of the breach of confidence action in such cases,[161] and some even allow HIPAA in through the "back door," establishing a standard of care in negligence *per se* cases.[162]

For example, *Resnick v. AvMed, Inc.*[163] concerned two unencrypted laptops that were stolen from the defendant managed care company. The compromised data concerned 1.2 million persons, some of whom subsequently became victims of identity theft. Dealing with Florida law allegations of breach of contract, breach of implied contract, breach of the implied covenant of good faith and fair dealing, and breach of fiduciary duty, the Eleventh Circuit addressed the question whether plaintiffs had alleged a sufficient nexus between the data theft and the identity theft. The court concluded that the plaintiffs had "pled a cognizable injury and . . . sufficient facts to allow for a plausible inference that AvMed's failures in securing their data resulted in their identities being stolen. They have shown a sufficient nexus between the data breach and the identity theft beyond allegations of time and sequence."[164] Overall there seems to be a proliferation of data breach cases filed in state courts.[165]

---

155. Medical Records Privacy Act, TEX. HEALTH & SAFETY CODE ANN. § 181.001(b)(2) (West 2010 & Supp. 2012).

156. *Id.* at § 181.152.

157. *Id.* at § 181.153.

158. *See supra* note 20 and accompanying text.

159. Acara v. Banks, 470 F.3d 569, 572 (5th Cir. 2006); Johnson v. Quander, 370 F. Supp. 2d 79, 99-100 (D. Colo. 2005).

160. *See, e.g.*, CAL. CIV. CODE § 56.36(b) (2013).

161. *See, e.g.*, Biddle v. Warren Gen. Hosp., 715 N.E.2d 518 (Ohio 1999).

162. *See, e.g.*, I.S. v. Wash. Univ., 2011 WL 2433585, at *2-3, 9 (E.D. Mo. 2011).

163. 693 F.3d 1317, 1321-22 (11th Cir. 2012).

164. *Id.* at 1330.

165. *See, e.g.*, Scott Graham, *Data Breach Cases Vex Health Care Sector*, THE RECORDER (Sept. 20, 2013),

State privacy case law[166] and legislation[167] are continually evolving both in and out of the health care space. However, there is reason to believe that health privacy exceptionalism remains an accepted tenet among state courts and legislatures.

C. Exceptionalism at the Federal Level

While the ethical basis (autonomy) for exceptional protection for health privacy is robust,[168] a strong legal basis for health privacy exceptionalism is harder to articulate. The U.S. Constitution is silent on the issue although the decisional privacy cases do recognize limited penumbral privacy claims.[169] *Whalen v. Roe* did articulate the duality of informational and decisional privacy in a case that, broadly at least, concerned health privacy.[170] Yet Justice Stevens' broadest pro-privacy statement in *Whalen* failed to articulate any exceptional treatment of health information.[171] Of course, in *Jaffee v. Redmond*, the same Justice recognized a broad federal common law psychotherapist privilege rooted in confidence and trust,[172] yet it was hardly exceptional as it was analogized to the spousal and attorney-client privileges.[173] More recently, the Supreme Court, while restraining

---

http://www.law.com/jsp/ca/PubArticleCA.jsp?id=1202620223375&Data_Breach_Cases_Vex_Health_Care_Sector.

166. *See, e.g.*, Tyler v. Michaels Stores, Inc., 984 N.E.2d 737, 747 (Mass. 2013) (noting Massachusetts law limits collection of personal identification data extended to a store collecting zip codes during credit card transaction (when not required by issuer)). *See also* Press Release, State of Conn., Office of the Att'y Gen., *Attorney General Announces $7 Million Multistate Settlement With Google Over Street View Collection of WiFi Data* (March 12, 2013), http://www.ct.gov/ag/cwp/view.asp?Q=520518. *Cf.* Siegler v. Best Buy Co. of Minn. Inc., 519 F.App'x 604, 604-05 (11th Cir. 2013) (holding that the retailer was not liable under the federal Driver's Privacy Protection Act for collecting information from customers' driver's licenses when they returned goods).

167. *See, e.g.*, CAL. FIN. CODE § 4052.5 (2013) (requiring explicit consent from the consumer for disclosure of financial information). *See also* VT. STAT. ANN. tit. 8, §§ 10203-04 (2013).

168. TOM L. BEAUCHAMP & JAMES F. CHILDRESS, PRINCIPLES OF BIOMEDICAL ETHICS 103-05 (6th ed. 2009).

169. *See, e.g.*, Griswold v. Connecticut, 381 U.S. 479, 483-85 (1965); Planned Parenthood of Cent. Mo. v. Danforth, 428 U.S. 52, 52, 60-61 (1976).

170. 429 U.S. 589, 599-600 (1977).

171. *Id.* at 605.

172. 518 U.S. 1, 2-3 (1996).

173. *Id.* at 10.

some aspects of the surveillance state,[174] generally has favored data liquidity over data protection.[175]

Outside of the health-related HIPAA, the Genetic Information Nondiscrimination Act of 2008 (GINA),[176] and a few other narrow sector-specific statutes like GLBA, most federal privacy law is quite general in its reach. For example, the Privacy Act of 1974, while applicable to health care data collected by the federal government, does not seem to apply exceptionally.[177] The same can be said of federal scrutiny of the privacy standards of private, non-health care entities. In this general space the FTC asserts two types of claims under Section 5(a) of the Federal Trade Commission Act: "unfair or deceptive acts or practices in or affecting commerce."[178] Thus, with regard to privacy, an unfair business practice case might be brought against a business for, say, failing to have adequate security, while a deceptive or misleading claim might apply to a business that, say, failed to comply with its own stated privacy policy. The FTC will leave most health care privacy cases to the HHS Office of Civil Rights[179] although it has asserted its jurisdiction in cases involving non-HIPAA entities. For example, *In the Matter of CBR Systems, Inc.*, the FTC entered into a settlement with a provider of umbilical cord blood and umbilical cord tissue-banking services. The proceeding

174. United States v. Jones, 132 S. Ct. 945, 949 (2012).

175. Sorrell v. IMS Health, Inc., 131 S.Ct. 2653, 2656-58 (2011) (striking down Vermont statute that restricted the sale and use of pharmacy records documenting prescribing practices of physicians).

176. Title I (applicable to health insurers) and Title II (applicable to employers and related entities) of GINA prohibit the use of genetic information in making insurance and employment decisions, restrict those entities from requesting, requiring or purchasing genetic information, and place limits on the disclosure of genetic information. Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110–233, 122 Stat. 881 (2008).

177. Privacy Act of 1974, Pub. L. No. 93–579, 88 Stat. 1896 (1974).

178. Federal Trade Commission Act, 15 U.S.C. § 45(a) (2012). *See also* § 45(n). *See generally* Complaint, FTC v. Wyndham Worldwide Corporation 2013 WL 1222491 (D. Ariz July 26, 2012), *available at* http://www.ftc.gov/os/caselist/1023142/120809wyndhamcmpt.pdf (bringing an against a hotel chain for failure to maintain adequate security for customer data).

179. *See generally Office for Civil Rights*, *supra* note 22. *See also* Memorandum of Understanding Between the FTC and Food & Drug Admin., MOU 225-71-8003 (1971), *available at* http://www.fda.gov/AboutFDA/PartnershipsCollaborations/MemorandaofUnderstandingMOUs/DomesticMOUs/ucm115791.htm.

related to the theft of unencrypted computer drives exposing the health information of almost 300,000 of the bank's customers.[180]

There has been little Congressional consideration of the implications of health privacy exceptionalism or, for that matter, its absence. A rare exception was at the 1999 hearings on GLBA. When it became apparent that health insurers would be covered by the proposed legislation, a provision was added with the intent to protect health data.[181] However, that provision would have had the unintended consequence of opening up health data to broad opt-out sharing among financial institutions with attendant secondary use risks. Organizations such as the American Medical Association[182] and the American Psychiatric Association (APA)[183] strongly voiced their concerns, and the provision was dropped from the final bill. The APA's Dr. Richard Harding argued before the House of Representatives, "It is critically important to recognize the difference between medical records privacy and financial privacy." He made the case for health privacy exceptionalism as follows:

> [T]he damages from breaches of medical records privacy are of a different nature. Medical records information can include information on heart disease, terminal illness, domestic violence, and other women's health issues, psychiatric treatment, alcoholism and drug abuse, sexually transmitted diseases and even adultery . . . .These disclosures can jeopardize our careers, our friendships, and even our marriages.
>
> And if such disclosures occur, there are truly few meaningful remedies. Seeking redress will simply lead to further dissemination of the highly private information that the patient wished to keep secret . . . .[184]

Just a few months later this model of health privacy exceptionalism was confirmed when President Clinton introduced the first version of the HIPAA privacy rule.[185] The rhetoric of

180. *Cbr Sys., Inc.*, File No. 1123120, 2013 WL 391859, at *13 (FTC Jan. 28, 2013).

181. Financial Services Act of 1999, H.R. 10, 106th Cong. § 351 (1999) (addressing the confidentiality of health and medical information).

182. *Financial Privacy: Hearing on H.R. 10 Before the Subcomm. on Financial Institutions and Consumer Credit of the Comm. on Banking and Financial Services,* 106th Cong. 97-98, 525-34 (1999) (statement of Donald J. Palmisano, M.D., J.D., A.M.A.).

183. *Id.* at 535-39 (statement of Richard Harding, M.D.).

184. *Id.*

185. Press Release, The White House, Remarks by the President on Medical Privacy (Oct. 29, 1999), http://archive.hhs.gov/news/press/1999pres/19991029b.html.

exceptionalism was clear. As the President noted, the purpose of the regulation was "to protect the *sanctity* of medical records," and it represented "an *unprecedented step* toward putting Americans back in control of their own medical records."[186]

Today the federal commitment to health privacy exceptionalism seems strong. Of course there were a couple of bumps in the road such as when the Bush Administration replaced the original Clinton Administration requirement of patient consent to disclosure for treatment, payment, or health care operations (TPO) purposes[187] with the more permissive statement that "[a] covered entity may obtain consent of the individual to use or disclose protected health information to carry out treatment, payment or health care operations."[188]

On the other hand the Bush Administration seemed to endorse health privacy exceptionalism when it championed the Genetic Information Nondiscrimination Act. GINA, signed into law by President Bush in May 2008, broadly prohibits discrimination by employers and health insurers based upon genetic information. It does so primarily by using an upstream data protection model whereby would-be data custodians are prohibited from collecting genetic information.[189]

Two recent federal government reports that have recommended the strengthening of data protection both recognize health privacy exceptionalism. Unfortunately, in doing so they may drive the unintended consequence of keeping strong, upstream protections out of the health care space.

First, the White House report *Consumer Data Privacy in a Networked World*,[190] while calling for Congress to enact legislation that includes an impressive Consumer Privacy Bill of Rights rotating around "Fair Information Practice Principles" (FIPPs), limits that proposal "to commercial sectors that are not subject to existing Federal data privacy laws."[191] Second, the FTC's *Protecting Consumer Privacy in an Era of Rapid Change*,[192] which calls for privacy by

186. *Id.* (emphasis added).

187. 45 C.F.R. § 164.506 (2001), *amended by* 45 C.F.R. § 164.506 (2009).

188. 45 C.F.R. § 164.506(b)(1) (2001).

189. Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110–233, 122 Stat. 881 (2008).

190. THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY, at i (2012) [hereinafter CONSUMER DATA PRIVACY], *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

191. *Id.*

192. FTC, *supra* note 96, at 1.

design and best privacy practices, expresses its sensitivity to burdens introduced by "overlapping or duplicative requirements on conduct that is already regulated" but more positively suggests the potential for the FIPPs framework to provide "an important baseline for entities that are not subject to sector-specific laws like HIPAA or GLBA."[193] Their considerable promise aside, neither report has led to legislation. And with the political classes closing ranks over the Big Data-tainted NSA spying controversy, a privacy law reform proposal does not seem likely to emerge from either the White House or Congress.[194]

IV. REFORMING HEALTH PRIVACY REGULATION IN THE FACE OF BIG DATA

Clearly big data challenges the core tenets of health privacy and its regulation.[195] As Viktor Mayer-Schönberger and Kenneth Cukier pithily note, "In the era of big data, the three core strategies long used to ensure privacy—individual notice and consent, opting out and anonymization—have lost much of their effectiveness."[196] Indeed, some of the big data implications for privacy are quite dramatic. First, the relative agnosticism of big data processing to either data size or data format radically reduces the traditional protective role of data friction. Second, big data predictive analytics do not content themselves with populations but increasingly operate on the individual level, thus challenging the core, autonomy-based privacy model. Third, big data nullifies core regulatory components such as de-identification or anonymization.[197] Fourth, and –for health privacy regulation –the most important effect, is the argument presented in this article: that big data increasingly will sidestep sector-based downstream health data protection by replicating that data with proxy data generated from data pools that are located in lightly regulated, HIPAA-free space.

193. *Id.* at 16-17.

194. *See generally* Gerry Smith & Ben Hallman, *NSA Spying Controversy Highlights Embrace Of Big Data*, HUFFINGTON POST (June 12, 2013), http://www.huffingtonpost.com/2013/06/12/nsa-big-data_n_3423482.html.

195. Terry, *Protecting Patient Privacy*, *supra* note 2, at 397.

196. MAYER-SCHÖNBERGER & CUKIER, *supra* note 124, at 156.

197. *See, e.g.*, Yves-Alexandre de Montjoye et al., *Unique in the Crowd: The Privacy Bounds of Human Mobility*, SCIENTIFIC REPS., Mar. 25, 2013, *available at* http://www.nature.com/srep/2013/130325/srep01376/pdf/srep01376.pdf .

While big data is only now attracting the attention of privacy advocates, its health-related businesses are in full flow. Clearly the big data model is attracting big claims. For example, in 2011 the McKinsey Global Institute estimated that "US health care could capture more than $300 billion in value every year, with two-thirds of that in the form of reductions to national health care expenditure of around 8 percent."[198]

For all the bold claims and notwithstanding the potential shown by the application of some big data technologies to health care, barriers remain. A recurring problem with the mapping of technological solutions to the U.S. health care model is that major progress depends on antecedent change by health care cultures, processes, precepts, and stakeholders.[199] In a 2013 report McKinsey & Company stated the big data challenge as follows:

> The old levers for capturing value—largely cost-reduction moves, such as unit price discounts based on contracting and negotiating leverage, or elimination of redundant treatments—do not take full advantage of the insights that big data provides and thus need to be supplemented or replaced with other measures related to the new value pathways. Similarly, traditional medical-management techniques will no longer be adequate, since they pit payors and providers against each other, framing benefit plans in terms of what is and isn't covered, rather than what is and is not most effective. Finally, traditional fee-for-service payment structures must be replaced with new systems that base reimbursement on insights provided by big data—a move that is already well under way.[200]

If nothing else, this anterior requirement for health care itself to change significantly before the power of big data can be fully leveraged may furnish a brief window in which to strengthen health privacy.

While many big data claims are the products of marketing frenzy, as yet another group of rent-seekers look to claim a piece of the health care economy, some contain a germ of truth. The next question then is the classic instrumental one: do the health care gains trump the privacy losses?

---

198. JAMES MANYIKA ET AL., MCKINSEY GLOBAL INST., BIG DATA: THE NEXT FRONTIER FOR INNOVATION, COMPETITION, AND PRODUCTIVITY 49 (2011), *available at* http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation.

199. *See* Terry, *supra* note 52, at 738-42. *See also* Nicolas P. Terry, *Pit Crews With Computers: Can Health Information Technology Fix Fragmented Care?*, 14 HOUS. J. HEALTH L. & POL'Y (forthcoming 2014).

200. GROVES ET AL., *supra* note 73, at 10.

A. Will Big Data Join the Instrumentalist Narrative?

Because of asserted positive claims made for big data, a fair question to ask is whether the benefits to health care should overcome (even if only partially) health privacy and its exceptional protections. Over the last decade and a half, as the HIPAA model of exceptional privacy has asserted itself, many involved in public health or biomedical research have supported a more utilitarian position. For example, Lawrence Gostin and James Hodge have argued that "[i]ndividuals should not be permitted to veto the sharing of personal information irrespective of the potential benefit to the public" and that "[p]rivacy rules should not be so arduous and inflexible that they significantly impede . . . health services research or surveillance . . ."[201]

However, the traditional rationales for privacy offer little room for an instrumentalist balancing of interests. Privacy claims traditionally have been based on quite absolutist claims of personhood, autonomy, property, control,[202] freedom from surveillance, protection from discrimination, or "hybrid inalienability."[203]

The physician-patient relationship was the font from which claims of privacy were derived. In this model privacy is a consequent or a component of autonomy. And, according to Tom Beauchamp and James Childress, in the ethical domain "[r]espect for autonomy is not a mere *ideal* in health care; it is a professional *obligation*. Autonomous choice is a *right* –not a *duty* –of patients."[204] For them privacy is part of the core autonomy "rights" bundle that must be protected as "the justification of the right to privacy parallels the justification of the right to give an informed consent . . . ."[205]

This autonomy model plays out as follows. The autonomous patient cedes control over (and/or property in) health data to the physician. The physician then becomes the patient's agent and either

201. Lawrence O. Gostin & James G. Hodge, Jr., *Personal Privacy and Common Goods: A Framework for Balancing under the National Health Information Privacy Rule*, 86 MINN. L. REV. 1439, 1441-42 (2002). *See also* Fred H. Cate, *Protecting Privacy in Health Research: The Limits of Individual Choice*, 98 CALIF. L. REV. 1765, 1770 (2010); Franklin G. Miller, *Research on Medical Records Without Informed Consent,* 36 J.L. MED. & ETHICS 560, 566 (2008). *Cf.* Mark A. Rothstein & Abigail B. Shoben, *Does Consent Bias Research?*, 13 AM. J. OF BIOETHICS 27 (2013).

202. *See* Vera Bergelson, *It's Personal But Is It Mine? Toward Property Rights in Personal Information*, 37 U.C. DAVIS L. REV. 379 (2003) (arguing for a broad (non-sector based) control-property model).

203. Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2060 (2004).

204. BEAUCHAMP & CHILDRESS, *supra* note 168, at 107.

205. *Id.* at 297-98.

is bound by the agent's duty of confidentiality in curating the patient's health data[206] or, according to Daniel Solove, may be liable for a confidence's betrayal.[207]

Not surprisingly, therefore, reformers wanting to see more health data made available for public health or research seek to undermine patient autonomy and the physician-patient relationship as foundational of health privacy (and indeed health privacy exceptionalism). For example, Roger Magnusson has argued that modern health privacy is less about the rights and obligations inherent in the physician-patient relationship and is more about "the power of the state as the broker for information flows within health care settings." He predicts that:

> Twenty years from now, it is by no means clear that the obvious starting point when considering health privacy law will be either the autonomy interests of health consumers or their treating physicians. What we now call health privacy laws are likely, at that time, to be less patient-focused, and to be described (and defended) with reference to the variety of aims that information policy, within the health sector, is designed to achieve.[208]

Calling out what he believes to be an artifact of a waning bilateral relationship, Magnusson predicts that more instrumental forces will recalibrate health privacy and, to put words into his mouth, reduce health privacy exceptionalism.

While it seems arguable that the continued industrialization of health care will deprecate the physician-patient relationship as a font of duties,[209] there are other, equally strong (or potentially stronger) rationales for privacy. For example, Edward Janger and Paul Schwartz argue for "constitutive privacy" whereby "[a]ccess to personal information and limits on it help form the nature of the society in which we live and shape our individual identities."[210] Although they seem to admit of considerable balancing at work in their model, this is not merely a relabeled utilitarian justification for turning over private information. Although Janger and Schwartz were primarily discussing the GLBA their constitutive privacy concept seems even stronger in the health care sector. They were also impressively prescient about big data, noting more than a decade ago:

206. *See generally* Terry, *supra* note 4.

207. Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 527 (2006).

208. Roger S. Magnusson, *The Changing Legal And Conceptual Shape Of Health Care Privacy*, 32 J.L. MED. & ETHICS 680, 681 (2004).

209. Terry, *supra* note 4, at 17.

210. Janger & Schwartz, *supra* note 135, at 1251.

> A financial institution knows whether a customer has recently bought running shoes or other consumer products, the name of one's physicians (as well as the nature of their specialty), and whether one has purchased orthotics or aspirin or other kinds of health care products. Some of this information might be embarrassing, and some of it might create potentially damaging labels for persons or lead to other harmful results. The cumulative impact of these disclosures can have a profound impact on the society in which we live. Regulatory attention is needed to control the resulting patterns of data accumulation and use.[211]

As the big data debate heats up it is likely that public health and research interests will join the data-brokers and the purveyors of BI in making instrumental arguments for data liquidity. Implied consent or opt-out rules will be proposed as the preferable operational rules. It will take a considerable effort to maintain the health privacy exceptionalism we currently enjoy let alone to promote new upstream controls on the data-brokers.

B. The Unlikely Alternative of Self-Regulation

In *Predictive Analytics* Eric Siegel discusses medically inflected data in the context of both the well-known story of Target Corporation's use of predictive analytics to identify potential customers in their second trimester of pregnancy[212] and his own research into the (apparently benign) practice of a health insurance company that predicted customer deaths so as to trigger end-of-life counseling.[213] He concludes:

> It's not what an organization comes to know; it's what it *does* about it. Inferring new, powerful data is not itself a crime, but it does evoke the burden of responsibility. Target does know how to benefit from pregnancy predictions without actually divulging them to anyone . . . . But any marketing department must realize that if it generates quasi-medical data from thin air, it must take on, with credibility, the privacy and security practices of a facility or department commonly entrusted with such data. *You made it, you manage it.*[214]

211. *Id.* at 1253.

212. Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES (Feb. 16, 2012), *available at* http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=all.

213. SIEGEL, *supra* note 74, at 64-65.

214. *Id.* at 65.

It also seems to be the FTC position that "with big data comes big responsibility. Firms that acquire and maintain large sets of consumer data must be responsible stewards of that information."[215] Unfortunately there is little or no evidence that the big data industry has either recognized or accepted any such "made it, manage it" mantra. It is at least as likely that these data custodians think of data protection as merely creating friction at a time when their businesses are thriving on data liquidity.

In late 2012 Senator John Rockefeller opened an investigation into information brokers,[216] following in the footsteps of Representatives Edward Markey and Joe Barton who had sent letters of inquiry to industry members.[217] The acting chief executive of the Direct Marketing Association subsequently characterized the senator's investigation as "a baseless fishing expedition." [218]

The indications are that the FTC also is skeptical that any exhortation to self-regulation or best data practices will be sufficient. In late 2012 the agency sent subpoenas to a range of data brokers seeking to learn "the nature and sources of the consumer information the data brokers collect" and "the extent to which the data brokers allow consumers to access and correct their information or to opt out of having their personal information sold."[219] The FTC increased the pressure in March 2013 when it sent warning letters to ten data brokers. These alerted the recipients of possible violations of the Fair Credit Reporting Act,[220] such as selling consumer information for use in making insurance or employment decisions without the appropriate safeguards.[221]

---

215. Ramirez, *supra* note 82, at 6.

216. Natasha Singer, *Senator Opens Investigation of Data Brokers*, N.Y. TIMES (Oct. 10, 2012), *available at* http://www.nytimes.com/2012/10/11/technology/senator-opens-investigation-of-data-brokers.html?_r=0.

217. Natasha Singer, *Congress to Examine Data Sellers*, N.Y. TIMES (July 24, 2012), *available at* http://www.nytimes.com/2012/07/25/technology/congress-opens-inquiry-into-data-brokers.html.

218. *Id.*

219. Press Release, FTC, FTC to Study Data Broker Industry's Collection and Use of Consumer Data: Comm'n Issues Nine Orders for Information to Analyze Industry's Privacy Practices (Dec. 18, 2012), http://www.ftc.gov/opa/2012/12/databrokers.shtm.

220. 15 U.S.C. § 1681 (2012) (listing the exclusive grounds whereby "a consumer reporting agency may furnish a consumer report").

221. Press Release, FTC, FTC Warns Data Broker Operations of Possible Privacy Violations (May 7, 2013), http://www.ftc.gov/opa/2013/05/databroker.shtm.

C. The Case for a New Upstream Data Protection Model

Distinct from the rationale for data protection are data protection's persistent functional and taxonomical problems. Daniel Solove has suggested a "harmful activities" taxonomy with four components: "(1) information collection, (2) information processing, (3) information dissemination and (4) invasion."[222] I prefer a broadly consistent classification –consistent because it, too, rotates around the data acquisition, processing, and disclosure timeline. Hence I make a broad distinction between upstream ("privacy") and downstream ("confidentiality") data protection models.

The former cluster includes both processes or rules designed to reduce the value or threat of data (such as imposing inalienability or requiring de-identification) and requirements that place formal limitations on data collection such as prohibitions on the collection of certain data such as genetic information or contextual rules that, say, prohibit the collection or retention of any data other than that necessary for the transaction in question. The latter, downstream protective cluster includes security requirements specifying physical and technological barriers to protect collected data, restrictions on the retention, disclosure, or distribution of collected information (for example to certain persons or for certain purposes) and notification of breach rules when the data has been compromised.

Obviously HIPAA was and is a downstream confidentiality model. Regulatory tweaks and the HITECH statutory modifications may have created a better mousetrap but have not deviated from that commitment to downstream data protection. Indeed, HITECH went further in the direction of downstream protection with its new breach notification duty.[223] The question is whether a mature confidentiality rule abetted by breach notification can cabin big data and thus maintain health privacy exceptionalism.

The core problem is that downstream, disclosure-centric models are highly dependent on the context of the original data grant. For example, a patient provides data (for example, via a physical examination) for the purposes of better informing his or her care team. Given that context it should be relatively easy to draw the line (or understand the scope of the consent) as to the line between appropriate and inappropriate disclosures by the health care providers. Thus, given the context we can understand the primary uses of the data and cast doubt on most calls on the same data for "secondary" uses.

In contrast, when there is no disclosure context, as is the case when a data-broker creates a medical data proxy of the patient using a variety of sources, it is very difficult to draw the non-disclosure line

222. Solove, *supra* note 207, at 488.

223. *See generally supra* notes 42-44 and accompanying text.

or operationalize meaningful consent. This is also true of indeterminate or intermediated data collection (for example, acquisition of data through third parties). As a result, data-brokers either discourage any regulation or seek to minimize government interference by nudging any regulation in the direction of a highly permissive consumer opt-out.[224]

When disclosure (downstream) regulation becomes compromised (as HIPAA has by data proxies) we must explore the potential for constraining the supply of big data to the data-brokers with a collection (upstream) model. As recently noted by FTC Chairwoman Edith Ramirez,

> As important as they are, use restrictions have serious limitations and cannot, by themselves, provide effective privacy protection. Information that is not collected in the first place can't be misused. And enforcement of use restrictions provides little solace to consumers whose personal information has been improperly revealed. There's no putting the genie back in the bottle.[225]

The White House's 2012 Consumer Privacy Bill of Rights lists seven Fair Information Practices Principles (FIPPs)[226] including two that primarily are upstream limitations: Individual Control and Respect for Context. The former is explained as a consumer "right to exercise control over what personal data companies collect from them and how they use it." The latter is explained as a consumer "right to expect that companies will collect, use and disclose personal data in ways that are consistent with the context in which consumers provide the data."[227] In the U.S. the successful fashioning of legal models to protect against data collection has been rare –a notable exception being the inalienability rule in GINA. However, other jurisdictions have been more successful. The original EU data protection directive nodded in the direction of health privacy exceptionalism, recognizing special protection for a sub-set of data including health.[228] The

224. *See* Natasha Singer, *A Data Broker Offers a Peek behind the Curtain*, N.Y. TIMES (Aug. 31, 2013), *available at* http://www.nytimes.com/2013/09/01/business/a-data-broker-offers-a-peek-behind-the-curtain.html?hp=&adxnnl=1&adxnnlx=1378046196-x6G6L6Bn65czQyL8dCiCyw&_r=3&.

225. Ramirez, *supra* note 82, at 6.

226. CONSUMER DATA PRIVACY, *supra* note 190, at 47-48.

227. *Id.* at 15.

228. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data , 1995 O.J. (L 281) 31-50 ("Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions,

directive also provided for upstream protection in addition to regulating disclosures. Thus, data collection must be collected for legitimate purposes and not retained for unrelated purposes.[229] The EU's new draft data protection regulation doubles down on such protections[230] but supplements regulatory protections with a property rights remedial model.[231] This would be particularly beneficial in a typical medically inflected big data scenario. Assume, for example, that a data broker collected supermarket or other sales data and developed a big data proxy for a person. Assume further that the person had consented at, say, a point of sale to the original collection of that data. Under the draft regulation the data subject's privacy rights would run with the data and subsequently the subject could demand that the data broker destroys the data.[232] In addition there are specific rights with regard to data that are used for marketing that likely would reduce the interest of the business consumers of big data in segmentation.[233]

Notwithstanding this insight into the realms of the possible (and the likely extraterritorial application of the regulation on U.S. businesses that touch EU data subjects) the development of upstream privacy legislation has slowed. Without federal action (and exactly how the FTC proceeds in its investigations of data-brokers will be a key barometer) we will likely see some states swatting at big data symptoms. While outright state bans on data collection are unlikely given the chilling effect of *Sorrell v. IMS Health, Inc.*,[234] states may require increasingly disclosive privacy policies as exemplified by the proposed amendment to the California law[235] that would require data

religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life."). *Id.* (providing a limited exception for health care providers).

229. *Id.*

230. Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, COM (2012) 11 final (Jan. 25, 2013), *available at* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

231. *See generally* Jacob M. Victor, *The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy*, 123 YALE L.J. 513 (2013).

232. Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, COM (2012) 11 final (Jan. 25, 2013), *available at* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

233. *Id.*

234. 131 S.Ct. 2653, 2656-58 (2011).

235. CAL. BUS. & PROF. CODE § 22575 (West 2012).

collectors to disclose their responses to signals such as those from a web browser requesting "do not track."[236]

Achieving either broad (controls on collection) or narrow (for example, disclosure of collection practices) limitations on big data collection likely will require both regulation and industry adherence to best practices consistent with the FTC's "privacy by design" model.[237] Of course it is probable that if legislation *is* passed to give life to the Consumer Privacy Bill of Rights it will be of general applicability and not limited to health data. Indeed, one of the challenges for reformers will be to avoid the exclusion of health data based upon its existing regulatory models.[238] The reality (indeed the *necessity*) is that HIPAA's downstream model can co-exist with a new upstream regulatory model. That is the best model for both guaranteeing health privacy's continued exceptional treatment and limiting the growth of big data proxies.

CONCLUSION

There is little doubt about how the big data industry and its customers wish any data privacy debate to proceed. In the words of a recent McKinsey report, the collective mindset about patient data needs to be shifted from "protect" to "share, with protections." Yet any conceded "protections" fall far short of what is necessary and what patients have come to expect given our history of health privacy exceptionalism. Indeed, some of the specific recommendations are antithetical to our current approach to health privacy. For example, the report suggests encouraging data sharing and streamlining consents, specifically that "data sharing could be made the default, rather than the exception."[239] However, McKinsey also noted the privacy-based objections that any such proposals would face:

> [A]s data liquidity increases, physicians and manufacturers will be subject to increased scrutiny, which could result in lawsuits or other adverse consequences. We know that these issues are already generating much concern, since many stakeholders have told us that their fears about data release outweigh their hope of using the information to discover new opportunities.[240]

236. Assemb. B. 370, Reg. Sess. (Cal. 2013), *available at* http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140AB370.

237. FTC, *supra* note 96, at 16-17.

238. *See supra* text accompanying notes 42-48.

239. GROVES ET AL., *supra* note 73, at 13.

240. *Id.*

Speaking at a June 2013 conference FTC Commissioner Julie Brill acknowledged that HIPAA was not the only regulated zone that was being side-stepped by big data as "new-fangled lending institutions that forgo traditional credit reports in favor of their own big-data-driven analyses culled from social networks and other online sources."[241] With specific regard to HIPAA privacy and, likely, data proxies, the Commissioner lamented:

> [W]hat damage is done to our individual sense of privacy and autonomy in a society in which information about some of the most sensitive aspects of our lives is available for analysts to examine without our knowledge or consent, and for anyone to buy if they are willing to pay the going price.[242]

Indeed, when faced with the claims for big data, health privacy advocates will not be able to rely on *status quo* arguments and will need to sharpen their defense of health privacy exceptionalism, while demanding new upstream regulation to constrict the collection of data being used to create proxy health data and sidestep HIPAA. As persuasively argued by Beauchamp and Childress, "We owe respect in the sense of deference to persons' autonomous wishes not to be observed, touched, intruded on and the like. The right to authorize access is basic."[243]

Of course one approach to the issue is to shift our attention to reducing or removing the incentives for customers of predictive analytics firms to care about the data. Recall how Congress was sufficiently concerned about how health insurers would use genetic information to make individual underwriting decisions that it passed GINA, prohibiting them from acquiring such data. Yet, today some (but not all) arguments for such genetic privacy exceptionalism seem less urgent given that the ACA broadly requires guaranteed issue and renewability,[244] broadly prohibiting pre-existing condition exclusions or related discrimination.[245] A realistic long-term goal must be to

241. Brill, *supra* note 1, at 4.

242. *Id.* at 8.

243. BEAUCHAMP & CHILDRESS, *supra* note 168, at 298.

244. *See* KAISER FAMILY FOUND., HEALTH INSURANCE MARKET REFORMS: GUARANTEED ISSUE 1 (2012), *available at* http://kaiserfamilyfoundation.files.wordpress.com/2013/01/8327.pdf; *see also* Press Release, U.S. Dep't Health & Human Servs., Health Care Law Protects Consumers Against Worst Insurance Practices (Feb. 22, 2013), http://www.hhs.gov/news/press/2013pres/02/20130222a.html.

245. Patient Protection and Affordable Care Act of 2010, Pub. L. No. 111-148, § 1201, 124 Stat. 146 (2010) (amending the Public Health Service Act §§ 2701, 2702, 2704 to prohibit pre-existing condition exclusions, discriminatory premium rates and requiring guaranteed availability of insurance coverage). *See also* Patient Protection and Affordable Care

reduce disparities and discrimination and thereby minimize any incentive to segment using data profiling.

A medium-term but realistic prediction is that there is a politically charged regulatory fight on the horizon. After all, as Mayer-Schönberger and Cukier note, "The history of the twentieth century [was] blood-soaked with situations in which data abetted ugly ends."[246] Disturbingly, however, privacy advocates may not like how that fight likely will turn out. Increasingly, as large swathes of the federal government become embroiled in and enamored with big data-driven decision-making and surveillance, so it may become politically or psychologically difficult for them to contemplate regulating mirroring behavior by private actors.[247]

On the other hand the position that we should not be taken advantage of without our permission could gain traction resulting in calls such as those expressed herein for increased data protection. Then we will need to enact new upstream data protection of broad applicability (i.e., without the narrow data custodian definitions we see in sector-based privacy models). Defeat of such reform will leave us huddled around downstream HIPAA protection, an exceptional protection but increasingly one that is (in big data terms) too small to care about and that can be circumvented by proxy data produced by the latest technologies.

Act; Health Insurance Market Rules; Rate Review, 78 Fed. Reg. 13,406 (Feb. 27, 2013) (to be codified at 45 C.F.R. pts. 144, 147, 150, 154, 156).

246. MAYER-SCHÖHNBERGER & CUKIER, *supra* note 124, at 151.

247. *See generally* Ashkan Soltani, *Soaring Surveillance: Technical, Not Legal, Constraints Determine The Scope of U.S. Government Surveillance,* MIT TECH. REV. (July 1, 2013), http://www.technologyreview.com/view/516691/technology-not-law-limits-mass-surveillance; Jill Lepore, *The Prism: Privacy in an Age of Publicity*, THE NEW YORKER (June 24, 2013), http://www.newyorker.com/reporting/2013/06/24/130624fa_fact_lepore; James Risen & Nick Wingfield, *Web's Reach Binds N.S.A. and Silicon Valley Leaders,* N.Y. TIMES (June 19, 2013), http://www.nytimes.com/2013/06/20/technology/silicon-valley-and-spy-agency-bound-by-strengthening-web.html?pagewanted=all&_r=0; James Risen & Eric Lichtblau, *How the U.S. Uses Technology to Mine More Data More Quickly*, N.Y. TIMES (June 8, 2013), http://www.nytimes.com/2013/06/09/us/revelations-give-look-at-spy-agencys-wider-reach.html?pagewanted=all.