March 2016

The Quantified Self Movement: Legal Challenges and Benefits of Personal Biometric Data Tracking

Timothy S. Hall

THE QUANTIFIED SELF MOVEMENT: LEGAL CHALLENGES AND BENEFITS OF PERSONAL BIOMETRIC DATA TRACKING

Timothy S. Hall[*]

In 2009, Google revealed a "flu trends" feature on its website.[1] Using aggregate search data from its users, the search engine company discovered that it could accurately detect seasonal influenza outbreaks by comparing its algorithm's estimates of influenza outbreaks derived from instances of health-related web searches with actual data from the Centers for Disease Control and Prevention.[2] The individual searches of millions of users of the World Wide Web, acting individually and with no thought of coordination, produced a data set that, when interpreted properly, generates a very useful tool for public health policymakers and healthcare providers.[3]

Others have developed social-media tools and techniques for helping individuals achieve personal goals, such as weight-loss or other health targets.[4] These tools work on the premise that one is more likely to achieve a goal, or stick to a plan, when others know about the goal and when the individual is part of a larger community dedicated to helping him or her achieve the goal.

The potential benefits of health-related data tracking and data mining are vast and expanding. At the macro level, there can be benefits in using the aggregated data of millions of individuals to predict health risks and disease outbreaks. These data can potentially improve public

---

* Professor of Law and Associate Dean for Academic Affairs, University of Louisville Louis D. Brandeis School of Law. Thanks to Jim Chen for generous research support during his years as Dean of the Brandeis School of Law, and to Lars Smith for helpful insights in discussion about this and related topics.

1. *Google Flu Trends*, GOOGLE.ORG, http://www.google.org/flutrends/about/how.html (last visited Aug. 11, 2014).
2. Jeremy Ginsberg et al., *Detecting Influenza Epidemics Using Search Engine Query Data*, 457 NATURE 935, 1012-14 (2009).
3. *Id.* at 1013-14.
4. *See, e.g.*, STICKK, http//www.stickk.com (last visited Aug. 11, 2014).

health responses to such outbreaks, save lives, and improve efficiency of service delivery. At the same time, at the micro level, collecting, sharing, and analyzing of individual health data can both improve health outcomes for those involved in the data collection and provide those individuals with a level of insight about their health-related behaviors that is not easily achievable through other means.

We are currently in the midst of a convergence of personal technology and health informatics. Advances in portable computing, the near-ubiquity of the smartphone with its app-driven marketing structure, the availability of high-speed mobile internet connectivity, and the rise of "cloud-based" computing services – both data storage and data processing, analysis, and mining – have enabled the emergence of a cluster of health-related data collection and tracking apps, devices, and services. These include nutritional tracking apps, weight management devices and apps, pedometers which track the user's movement and calculate the health effects of one's exercise (or lack thereof), wristbands which purport to measure the quality of one's sleep, and others too numerous to list here. This practice of personal data tracking and analysis is often referred to as the "Quantified Self" movement, or as "Life-Logging" or "Life-Hacking."[5] Currently, health-tracking apps primarily rely on the manual input of data from the user, with some exceptions. This is starting to change with the advent of devices that measure health parameters directly from the individual user.[6] However, commentators predict that in the near future, there will be sensors – perhaps implantable or wearable sensors – that will send streams of biometric data from the individual user to a smartphone to create a database of information to monitor potential adverse health events.[7] These sorts of uses of mobile computers such as smartphones have not gone unnoticed by makers of the devices. As of this writing, Apple redesigned its flagship smartphone, the iPhone 5s, with a "motion

5. The "Quantified Self," "Life-Logging," or "Life-Hacking" movements and communities are not limited to collection and aggregation of health data. One can find websites, apps, and online discussions devoted to data-driven analysis of virtually every aspect of modern life: from workplace productivity to personal confidence to memory improvement. *See, e.g.*, LIFEHACKER, http://www.lifehacker.com (last visited Aug. 11, 2014). However, for purposes of this roundtable on the intersection of healthcare law and intellectual property law, this article focuses on devices and applications that collect health-related or biometric data.

6. *See, e.g.*, *Smart Body Analyzer*, WITHINGS, http://www.withings.com/us/smart-body-analyzer.html (last visited Aug. 11, 2014) (the Withings wireless bathroom scale measures not only weight, but also body fat and muscle mass percentages).

7. *See* ERIC TOPOL, THE CREATIVE DESTRUCTION OF MEDICINE 162-63 (2012) (describing hypothetical nanosensor monitoring of patients' blood to detect markers of heart disease or cancers for those at high risk of such diseases).

coprocessor."[8] One of the stated purposes of including this specialty chip in the iPhone is to enable increased use of the device for fitness and health purposes, in part by reducing the load of such tracking programs on the main processor, and thus battery life, of the device.[9]

Proponents of these devices and apps both envision a near future in which individuals will have a level of information about and control over their daily lives unequalled in human history.[10] They predict that this unprecedented exercise of healthcare consumer autonomy will have dramatic effects on the way in which healthcare is practiced, virtually ending the practice of medicine as we know it.[11]

This article explores some of the potential pitfalls associated with collection of detailed individual biometric or health-related information, and demonstrates that current laws and regulations are not well designed to protect users of these devices and apps from unauthorized use or misuse of their data. Health information is among the most sensitive, intimate, and potentially damaging personal information one may possess, and health policymakers have made health information privacy a priority for decades for good reason. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was one of the major health policy legislative achievements of the 1990s[12] However, HIPAA is of no value for the protection of individually collected biometric data of the sort discussed here.

HIPAA generally prohibits unauthorized disclosures of protected health information except for a legitimate medical, business, or public health use as defined in the statute and regulations.[13] However, there are two problems with applying HIPAA to individually collected biometric information. First, by its terms, HIPAA only applies to so-called "Covered Entities."[14] While health plans, healthcare providers, and healthcare clearinghouses must follow HIPAA regulations, companies or others who aggregate individuals' biometric data as part of a health behavior tracking app are not "Covered Entities" under HIPAA, as they

8. *iPhone 5s Tech Specs*, APPLE, http://www.apple.com/iphone-5s/specs/ (last visited Aug. 11, 2014).

9. *See* Matthew Miller, *Apple iPhone 5s review: The Best Gets Better*, ZDNET (Nov. 12, 2013), http://www.zdnet.com/apple-iphone-5s-review-the-best-gets-better-7000023092/.

10. *See* TOPOL, *supra* note 7.

11. *Id.* at 178-95.

12. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-91, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 18, 26, 29, & 42 U.S.C.) [hereinafter HIPAA].

13. *See id.* at § 1173(d)(2), 42 U.S.C.A. § 1320d-2 (Westlaw through P.L. 113-25 (excluding P.L. 113-21)).

14. *Id.*

are not healthcare providers.[15] Second, HIPAA was written to apply primarily to medical records generated by "Covered Entities."[16] As a result, the definition of "[i]ndividually identifiable health information" in HIPAA is written to apply only to medical and billing records.[17] Thus, disclosure of individually identifiable biometric data by the company that manufactures the device, sells the app, or runs the website aggregating the data does not violate HIPAA's Privacy Rule as it currently stands.

Another potential source of regulation of devices and apps involving healthcare or medical uses is the Food and Drug Administration (FDA). The FDA recently issued a Guidance regarding the agency's approach to "mobile medical apps."[18] Although this document makes clear that the FDA is aware of the current boom in individually generated biometric information, the FDA does not currently plan to exercise its regulatory authority over many of the health-related apps currently on the market.[19]

The FDA Guidance establishes three categories of what it refers to as "mobile apps."[20] These categories are:

> 1. Apps that connect to a medical device to control the device or acquire data from the device;
> 2. Apps that "transform the mobile platform into a regulated medical device . . . including functionalities similar to those of currently regulated medical devices;" and
> 3. Apps that provide analysis, diagnosis or treatment recommendations specific to an individual patient.[21]

Such mobile apps will not fall under the current regulatory authority of the FDA because they do not meet the definition of a "medical device."[22] Also, even if a mobile app does meet the definition

15. 45 C.F.R. §§ 160.102-103 (2014). Even if they were healthcare providers, HIPAA protections only attach when a healthcare provider transmits health information electronically in connection with certain types of transactions. *Id.* at § 160.103.

16. *Id.*

17. *Id.*

18. U.S. DEPT. OF HEALTH & HUMAN SERV. FOOD & DRUG ADMIN., MOBILE MEDICAL APPLICATIONS: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF (2013) [hereinafter FDA Guidance].

19. *Id.* at 24 n.32.

20. *Id.* at 4 (defining "mobile apps" as "software applications intended for use on mobile platforms").

21. *Id.* at 14-15.

22. *Id.*

of a "medical device," the FDA will not exercise its regulatory authority over those apps because of the low risk they present to the public.[23] Finally, the FDA Guidance describes a category of mobile apps which are "medical devices" and which "pose a risk to the patient's safety if the mobile app were to not function as intended"[24] that the FDA does intend to regulate as medical devices. The FDA refers to these regulated apps as "mobile medical applications."[25]

The computing platform upon which a mobile app is executed is not a medical device manufacturer and will not be regulated by the FDA.[26] Similarly, the websites through which apps for these devices are sold, such as the Apple App Store or Google Play, are not considered manufacturers subject to the FDA's regulatory authority.[27]

Thus, while some apps that enable the collection of individually generated biometric information may also fall under the regulated category of "mobile medical apps," many more likely will not. Specifically, the FDA states that it does not currently intend to exercise regulatory authority over apps that "[p]rovide patients with simple tools to organize and track their health information."[28] More specifically, the types of apps over which the FDA intends to "exercise enforcement discretion" are listed in an appendix to the FDA Guidance.[29] These include many common health-tracking apps such as:

> Mobile apps that provide patients a portal into their own health information, such as . . . historical trending and comparison of vital signs;
>
> Mobile apps that allow a user to collect blood pressure data and share this data through email, track and trend it, or upload it to a personal or electronic health record; [and]
>
> Mobile apps that are intended for individuals to log, record, track, evaluate, or make decisions or behavioral suggestions related to developing or maintaining general fitness, health or

23. *Id.*

24. *Id.*

25. *Id.* at 7.

26. *Id.* at 10 ("[I]f it is possible to run mobile medical apps on BrandNamePhone but BrandNamePhone is not marketed by BrandNameCompany as intended for use as a medical device, then BrandNameCompany would not be considered a mobile medical app manufacturer or a medical device manufacturer.").

27. *Id.* at 10-11.

28. *Id.* at 16.

29. *Id.* at 24 n.32.

wellness[.][30]

It is apparent that, while certain apps will be regulated as medical devices,[31] many apps that allow collection, tracking, and sharing of personal health information will not. The FDA's regulatory focus is on the clinical functioning of the medical device app, not on protection of users from potential misuse of sensitive health and wellness information that may be generated, stored, tracked, or shared by such devices. Although the FDA may in the future decide to expand its exercise of regulatory authority over a wider array of health-related apps, FDA regulation today does not constitute a meaningful regulation of the data streams generated by the vast majority of these apps.

Turning from federal regulation to private law, unauthorized disclosure of individually generated biometric information may be a breach of contract between the device maker or app provider and the user. Can a user of the health behavior app or device make a claim for unauthorized disclosure of the data stream or database generated by that device? A comprehensive review of terms of service for health-tracking apps and devices is beyond the scope of this article. However, the terms of use of one of the most popular devices currently on the market, the FitBit range of "activity trackers," impose on the company only the obligation to adhere to the privacy settings selected by the user within the FitBit web site interface.[32] To the extent that the company fails to comply with the privacy settings selected by the user, a claim for breach of contract might lie. However, any such claim would be subject to the usual problems of proof of damages in contract cases, as well as to the foreseeability limitation on damages first articulated in the classic case of *Hadley v. Baxendale*, which limits consequential damages in breach of contract cases to those damages within the contemplation of the parties at the time the contract was entered into.[33]

If the information is intentionally taken by a third party, such as a malicious computer hacker, the user might assert a claim for conversion of his or her property. However, many jurisdictions do not permit a

30. *Id.*

31. An example of one such app is the AliveCor ECG device and associated app, which is a portable heart monitor that has been approved by the FDA. This device allows smartphone tracking of cardiac data and, through a companion app created by the University of Southern California, can link the user's heart rate to photographs taken with the smartphone. Timothy J. Seppala, *AliveCor ECG comes to Android*, ENGADGET (Oct. 4, 2013), http://www.engadget.com/2013/10/04/alivecor-android-ecg-biogram/.

32. *Website Terms and Conditions*, FITBIT, http://www.fitbit.com/terms (last updated Dec. 15, 2011).

33. *See* Hadley v. Baxendale, (1854) 156 Eng. Rep. 145; 9 Exch. 341, 354.

claim for conversion of intangible property.[34] In the few jurisdictions that do recognize such a claim, however, that claim still may not be available for the sort of data at issue here.[35]

New York recognized a cause of action for conversion of computer data in *Thyroff v. Nationwide Mutual Ins. Co.*.[36] In *Thyroff*, an insurance agency repossessed a computer leased to its agent upon termination of the agency agreement.[37] The computer contained personal data, including emails, in addition to business data.[38] The agent sued for conversion of the personal data contained in the computer.[39] The Court of Appeals of New York agreed with the agent that the tort of conversion should be modernized to cover intangible property such as computer data.[40] However, the data in *Thyroff* existed only on the single computer.[41] It was not "in the cloud." Thus, when Nationwide repossessed the computer, it deprived *Thyroff* of the ability to access the data.[42] The court's discussion of conversion in *Thyroff* does not make clear whether the court would agree that taking a copy of data, while leaving the original database still accessible to the user, would constitute conversion. For this reason, one cannot definitively say that a theft of personally identifiable biometric data from an app or website would be actionable as conversion.

Professor Lars Smith considered an analogous problem in his 2006 article, *RFID And Other Embedded Technologies: Who Owns the Data?*[43] Professor Smith, writing before the rise of individually collected biometric data, considered the problem of data contained in radio frequency identification (RFID) tags and read by RFID scanners.[44] Among other theories, he asks whether the theft of such data constitutes a violation of the Electronic Communications Privacy Act (ECPA).[45] Professor Smith concludes that while a violation of the ECPA may occur

---

34. *See, e.g.*, DIRECTV, Inc. v. Lockwood, 311 F. Supp. 2d 1147, 1150-51 (D. Kan. 2004) (denying conversion claim for alleged interception and decryption of satellite signals).

35. *See, e.g.*, Joe Hand Promotions, Inc. v. Lynch, 822 F. Supp. 2d 803, 809 (N.D. Ill. 2011) (denying conversion claim for television programming).

36. Thyroff v. Nationwide Mutual Ins. Co., 864 N.E.2d 1272, 1273 (N.Y. 2007).

37. *Id.*

38. *Id.*

39. *Id.*

40. *Id.* at 1278.

41. *Id.*

42. *Id.* at 1273.

43. Lars S. Smith, *RFID and Other Embedded Technologies: Who Owns the Data?*, 22 SANTA CLARA COMPUTER & HIGH TECH L.J. 695, 696 (2006).

44. *Id.* at 700-02.

45. *Id.* at 751-54.

if a third party intercepts the transfer of data between the device and the database, the data otherwise generated by the device is probably not an "electronic communication" for purposes of the ECPA.[46] If the data are not in transit, the information is not protected by the ECPA.[47] In addition, there is another potential hurdle to even this limited protection: the ECPA explicitly exempts "tracking devices."[48] A "tracking device" is defined as "an electronic or mechanical device which permits the tracking of the movement of a person or object."[49] While not applicable to apps that require manual input of the relevant data, mobile biometric data collection devices, such as FitBit "activity trackers,"[50] may be tracking devices under the ECPA and thus not covered by its provisions at all.

Much has been written about the changing perceptions of privacy in the digital age. Those of us in law school administration and student services have seen the potential dangers of such over-sharing when information damaging to the reputations of our students is accessed by potential employers or even bar admissions officials. In the quantified self-movement, there are diverse approaches to privacy. Some quantified self-advocates favor a curtailment of privacy (or perhaps a formal recognition that privacy rights on the Internet are in fact seriously curtailed), articulating a version of the "information wants to be free" meme.[51] Others take a more measured approach, trying to articulate standards and expectations for online and cloud-computing privacy. It is not unreasonable to believe that many users of biometric tracking apps and devices have higher expectations of privacy than current law provides.

Privacy may also be invaded through demands of law enforcement. Unlike the privacy issues discussed above, these privacy issues are governed by the Fourth Amendment to the United States Constitution, which protects against unreasonable searches and seizures.[52] With respect to Fourth Amendment claims arising out of disclosure of individually collected biometric data, the Third Party Disclosures doctrine might be interpreted to provide no protection to data stored on

46. *Id.* at 752-54.

47. *Id.* at 754.

48. *Id.* at 752-53 nn.285-87 (citing 18 U.S.C. §§ 2510(12)(C), 3117(b) (2000)).

49. *Id.*

50. *See* FITBIT, http://www.fitbit.com (last visited Aug. 11, 2014).

51. *See* R. Polk Wagner, *Information Wants to be Free: Intellectual Property and the Mythologies of Control*, 103 COLUM. L. REV. 995, 999 n.14 (2003) (attributing the quote to Stewart Brand).

52. U.S. CONST. amend. IV.

third party servers or "in the cloud."[53] The Third Party Disclosures, or "Knowing Exposure," doctrine provides that information which has been voluntarily disclosed to a third party is no longer subject to a reasonable expectation of privacy.[54] In 2010, Professor Christopher Slobogin noted that "[t]o date, the Supreme Court's interpretation of the Fourth Amendment has [both] failed to anticipate [the technological] revolution and continued to ignore it."[55] Recognizing that modern Fourth Amendment "search" jurisprudence started, in *Katz v. United States*, from the premise that non-physical interception of intangible communication could constitute a "search,"[56] Professor Slobogin demonstrates that subsequent reliance by the Court on the "reasonable expectations of privacy" test has "pretty much limited [*Katz*] to its facts."[57] The key problem for purposes of this article is language in *Katz* which states that "what a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[58] When *Katz* is read in light of subsequent decisions involving bank records and telephone systems, the conclusion drawn from Professor Slobogin's work is that it is highly unlikely that personal data stored on third party servers (that is, virtually all of the personal biometric data stored "in the cloud" and accessed via mobile devices) will be afforded Fourth Amendment protections against governmental search and examination.

Finally, we turn from unauthorized disclosure to authorized, even desired, disclosure and examine how even this may have troubling consequences. Many decisions affecting an individual, including but not limited to decisions about employment and insurability, may turn in part on information about the individual's health status. The availability of detailed personal biometric data about oneself may lead to a system in which there are incentives for what we might call "proverse selection" in information disclosure.[59] Proverse selection is the opposite of the more

---

53. *See* Orin S. Kerr, *The Case for the Third Party Doctrine*, 107 MICH. L. REV. 561, 563 (2009).

54. *Id.*

55. Christopher Slobogin, *Is the Fourth Amendment Relevant in a Technological Age?*, *in* CONSTITUTION 3.0: FREEDOM AND TECHNOLOGICAL CHANGE 12 (Jeffrey Rosen & Benjamin Wittes eds., 2011).

56. *Id.* at 13 (citing Katz v. United States, 389 U.S. 347 (1967)).

57. *Id.*

58. *Id.* at 14 (quoting *Katz*, 389 U.S. at 351).

59. *See* Scott Peppet, *The Quantified Self: Personal Choice and Privacy Problem?*, CONCURRING OPINIONS (NOV. 16, 2010), http://www.concurringopinions.com/archives/2010/11/the-quantified-self-personal-choice-and-privacy-problem.html.

familiar "adverse selection" problem in which individuals who know or suspect that they will need insurance are more likely to apply for it.[60] Adverse selection can skew an insurance pool such that premiums collected are not sufficient to pay claims. This leads to the classic insurance "death spiral" in which rising premiums chase rising claims until the insurer is bankrupted. [61]

Proverse selection works somewhat differently and operates as an incentive to reveal positive information about one's risk profile, even if not required (or, sometimes, even if prohibited). Even if not required by employers, might prospective employees want to share positive information about themselves? Might applicants for health insurance or life insurance want to demonstrate to prospective issuers that they in fact represent good risks?[62] Auto insurance customers are already given incentives by at least one insurer to allow that insurer to collect data on their driving habits.[63] Ultimately, if enough applicants for jobs or insurance are voluntarily offering positive information, this leads to an inference of negativity on the part of those not disclosing, even if that inference is unwarranted.

Ethicists and commentators have championed the "right not to know" in another health information context – that of genetic testing. While genetic testing may reveal useful information, it may also reveal information that is unusable, or that causes more anxiety or stress than is warranted. In extreme cases, knowledge of a potential, though unquantified, genetic risk may lead individuals to make poor medical treatment decisions. Although the collected data are of a different sort, the "right not to know" information, which may cause undue stress, anxiety, or even harm to certain individuals, should be taken as seriously in this context as in the genetic testing context.

This last concern about individual biometric tracking may seem far-fetched or unlikely, but so do some of the claims made for such data collection by its proponents. If the positive claims of writers such as

---

60. *See* Robert H. Jerry, II, *Health Insurer's Use of Genetic Information: A Missouri Perspective on a Changing Regulatory Landscape*, 64 MO. L. REV. 759, 770-71 (1999).

61. *See* Peter Siegelman, *Adverse Selection in Insurance Markets: An Exaggerated Threat*, 113 YALE L.J. 1223, 1223-24 (2004).

62. *See* Peppet, *supra* note 59.

63. *See* Becky Yerak, *Devices Map Your Driving Habits, can Help Save Money on Insurance Premiums*, CHICAGO TRIBUNE, Sept. 23, 2012, http://articles.chicagotribune.com/2012-09-23/business/ct-biz-0923-telematics—20120923_1_biggest-auto-insurers-insurance-products-claims-costs. Progressive Insurance reports more than $1 billion in policies were written using their SnapShot tracking device in the most recent fiscal year. *Id.*

Eric Topol are to be taken seriously,[64] then we should also take seriously the potential negative consequences of such a dramatic realignment of our current expectations and practices of healthcare data collection and service delivery. Perhaps one day the main source of health data will not be collected via large diagnostic machines in our doctors' offices and hospitals, but via nanosensors in our bloodstreams interacting wirelessly with the computers in our suit pockets. In 1890, Brandeis and Warren defined the right of privacy as the "right to be let alone."[65] Perhaps Brandeis' "right to be left alone" should be reconceptualized for the digital, cloud-driven, over-measured future as a "right to be unquantified."

Individualized biometric data tracking and analysis, while still in its infancy, holds great promise for improving both individual health and public health. However, as with other technological advances, the law may not keep up with technological capabilities without intentional intervention by scholars, legislatures, and courts. Existing common law and statutory law governing privacy in both electronic communication and healthcare data are not sufficient to ensure protection of individually collected biometric data. While some commentators decry emphasis on privacy as outmoded in light of new technologies, this article takes the position that the law should not force this loss of privacy on users of this technology, but should endeavor to protect a sphere of privacy from which individuals may depart of their own informed consent. Although concrete proposals for reform are beyond the scope and the allotted space of this essay, the need for attention to such reforms should be apparent.

64. *See* TOPOL, *supra* note 7.

65. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193-205 (1890).