University of Maine School of Law
University of Maine School of Law Digital Commons

Faculty Publications | Faculty Scholarship

Fall 2013

We Know Who You Are and What You Are Made Of: The Illusion of Internet Anonymity and Its Impact on Protection from Genetic Discrimination

Christine S. Davik
University of Maine School of Law, christine.davik@maine.edu

Follow this and additional works at: http://digitalcommons.mainelaw.maine.edu/faculty-publications

 Part of the Law Commons

Suggested Bluebook Citation

Christine S. Davik, *We Know Who You Are and What You Are Made Of: The Illusion of Internet Anonymity and Its Impact on Protection from Genetic Discrimination*, 64 Case W. Res. L. Rev. 17 (2013).
Available at: http://digitalcommons.mainelaw.maine.edu/faculty-publications/3

This Article is brought to you for free and open access by the Faculty Scholarship at University of Maine School of Law Digital Commons. It has been accepted for inclusion in Faculty Publications by an authorized administrator of University of Maine School of Law Digital Commons. For more information, please contact mdecrow@maine.edu.

Case Western Reserve Law Review

Volume 64 Fall 2013 Issue 1

We Know Who You Are and What You're Made Of: The Illusion of Internet Anonymity and Its Impact on Protection from Genetic Discrimination

Christine Suzanne Davik

We Know Who You Are and What You Are Made Of: The Illusion of Internet Anonymity and Its Impact on Protection from Genetic Discrimination

By Christine Suzanne Davik[†]

Abstract

Recent advances in technology allow the online activities of Internet users to be monitored, gathered, and recorded without their knowledge. New electronic tools can compile extensive data on exactly what an individual is doing on the Web. This information can then be almost simultaneously cross-referenced with additional data to create detailed dossiers, including the user's age, zip code, gender, and even health-related issues. While there is a vast amount of consumer information that can easily be accessed, at present there are very few restrictions on how the data amassed can be used. As a result, when consumers go online to search for medical knowledge or to find needed support, they risk providing marketers, data brokers, and, consequently, even employers with a host of sensitive information. Such a possibility is more than theoretical because comprehensive background screening reports currently exist that profile one's social media activities or participation in purportedly anonymous Internet discussion groups. Furthermore, even when Internet users take steps to conceal their online activities, job applicants are increasingly required to provide log-in information.

Apprehension over the potential for misuse of personal health information and genetic data by employers is not entirely new. In 2008, Congress enacted the Genetic Information Nondiscrimination Act (GINA), a law designed to provide protection from not only the utilization of genetic data and family health history in connection with employment-related decisions but also the initial acquisition of such data. However, when the Act and its regulations are examined

† Professor of Law, University of Maine School of Law; B.S. University of Illinois, 1992; J.D. University of Illinois, 1995. Many thanks to the participants at the 2012 Works-in-Progress Intellectual Property Colloquium held at Houston Law Center for extremely valuable comments and conversations. I am also grateful to Julie Welch for her exceptional research assistance. Additionally, I would like to thank Dean Peter Pitegoff and the University of Maine School of Law for financial support in the form of a summer research grant and sabbatical leave to work on this and other projects.

closely in light of advancements in the manner in which data is now gathered and the increasing ease with which seemingly anonymized data can be linked to a particular individual, only then do serious deficiencies become apparent. These defects must be corrected to alleviate patients' fears over obtaining genetic testing today due to their concerns regarding the use of their genetic information tomorrow.

CONTENTS

INTRODUCTION

Recently, there has been an astonishing increase in not only the pervasiveness but also the invasiveness of new computer technology that can monitor and chronicle Internet users' online activities without their knowledge.[1] These electronic tools can provide

1. *See, e.g.*, FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESS AND POLICYMAKERS, PRELIMINARY FTC STAFF REPORT (2010) [hereinafter FTC PRELIMINARY REPORT], *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf; Julia Angwin, *The Web's New Gold Mine: Your Secrets*, WALL ST. J., July 31, 2010, at W1 (detailing an investigation of the nation's fifty most widely used websites, which revealed that, on average, each site automatically and surreptitiously

instantaneous information on exactly what an individual is doing on the Web by surreptitiously recording extensive information regarding the computer user's keystrokes and mouse movements on a particular site. This information can then be almost simultaneously cross-referenced to provide additional data—often including the user's age, zip code, gender, income, and even health-related issues—to create detailed dossiers on individual computer users.[2] This is accomplished through computer software[3] that gathers the small bits of data individuals leave in a wide variety of places throughout cyberspace and then employs sophisticated algorithms that allow for this information to be linked to a particular person.

Information-gathering companies commonly argue that their actions are not an invasion of privacy because the individual pieces of data frequently obtained are not in and of themselves personally identifying.[4] However, this line of reasoning is increasingly less persuasive due, in significant part, to recent technological advances. For example, just a few years ago, a group of researchers from the University of Minnesota published a study describing how easy it has become for data-mining companies to create exceptionally detailed profiles of Internet users, even when they post information anonymously or pseudonymously.[5] Additionally, these scholars found that by using only three pieces of data Internet users commonly divulge when registering at a website (one's zip code, birth date, and gender), most Americans can be identified by name and address.[6]

Such data gathering has become big business and is only expected to continue growing. Spending on information from online sources is predicted to more than double from $410 million in 2009 to $840 million in 2012.[7] While there is now a vast amount of consumer data that can easily be purchased, at present there are very few restrictions on the use of such scraping and tracking devices to collect the information or, of arguably greater concern, how the amassed data

---

installed sixty-four pieces of tracking technology onto the computers of visitors).

2. Angwin, *supra* note 1.

3. *See infra* Part I.A (discussing the various computer technologies employed to conduct such monitoring and data gathering).

4. *See infra* Part I.B.4 (evaluating the various arguments of electronic data gatherers in defense of their electronic tracking).

5. *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1705 (2010) (discussing the research of Dr. Latanya Sweeney).

6. *Id.*

7. Julia Angwin & Steve Stecklow, "*Scrapers" Dig Deep for Data on Web,* WALL ST. J., Oct. 12, 2010, at A1.

can be utilized.[8] This is true even when it includes sensitive categories of information such as health-related data. Instead, information-gathering companies are left to develop their own seemingly incongruous policies. An example is Healthline Networks, Inc., one of the healthcare industry's leading providers of advertising services. Healthline does not track users viewing "sensitive topics" relating to eating disorders and impotence but admits to gathering data when individuals instead look up information on bipolar disorder, anxiety, and overactive bladders.[9]

Apprehension over the potential for misuse of personal medical information and genetic data is not, however, entirely new. By the time the international Human Genome Project had officially begun in 1990, with the stated goal of fully identifying the genes and determining the sequence of human DNA,[10] substantial concerns had already emerged about how such data might be utilized. This was particularly true in the context of employment and insurance-related decisions. Consequently, in the mid-1990s several bills were introduced in Congress in an attempt to alleviate the public's growing worries.[11] Research studies[12] showed that patients were increasingly

8. *See infra* Part I.B (examining the recently released FTC principles, the White House Report on Consumer Privacy, and several attempts in Congress to pass legislation in various forms to deal with such issues).

9. Angwin, *supra* note 1.

10. *See generally* U.S. DEP'T OF ENERGY GENOME PROGRAMS, http://genomics.energy.gov (last visited June 22, 2012) (providing detailed information on the Human Genome Project). The U.S. Human Genome Project was coordinated and sponsored by the U.S. Department of Energy and the National Institutes of Health. *Id.*

11. *See* Nat'l Insts. of Health, *Genetic Nondiscrimination Federal Legislation Archive*, GENOME, http://www.genome.gov/11510239 (last visited Feb. 24, 2013).

12. *See, e.g.*, Kira A. Apse et al., *Perceptions of Genetic Discrimination Among At-Risk Relatives of Colorectal Cancer Patients*, 6 GENETICS MED. 510 (2004) ("Findings from this study demonstrate the negative effect of concerns about genetic discrimination on decisions about utilization of genetic services. Stronger legislative protections against genetic discrimination and increased public education through the scientific community and media sources are needed."); Rachael Brandt et al., *Cancer Genetics Evaluation: Barriers to and Improvements for Referral*, 12 GENETIC TESTING 9 (2008) ("The largest barriers to referral were lack of program awareness and limited knowledge regarding patient eligibility, improved insurance coverage, and antidiscrimination legislation."); Mark A. Rothstein, *Is GINA Worth the Wait?*, 36 J.L. MED. & ETHICS 174, 175 (2008) ("There is considerable evidence that numerous individuals who are genetically at-risk for some serious disorders decline potentially efficacious genetic testing and medical intervention because they are concerned about the possibility of discrimination against themselves and family members."); Jeffrey N. Weitzel et al., *Genetics, Genomics, and Cancer Risk*

avoiding genetic testing and participating in related clinical trials due to fears of how test results might be used against themselves or family members.[13] This was problematic from a public health standpoint on numerous accounts. First, the information from such tests is often exceptionally helpful in taking preventive measures to minimize the likelihood of the occurrence of the disease in the first place. Additionally, at the onset of a disease, such data may be essential to making fully informed treatment decisions and provide for the possibility of lessening the severity of the now present condition. Moreover, without patients willing to enroll in research studies, future medical advancements could be considerably impeded.

Almost two decades after the first attempt to pass genetic non-discrimination legislation, the Genetic Information Nondiscrimination Act (GINA) was signed into law in May 2008, although it did not become fully effective until May 2010.[14] GINA prohibits not only the utilization of genetic information in connection with employment-

Assessment: State of the Art and Future Directions in the Era of Personalized Medicine, 61 CA: CANCER J. FOR CLINICIANS 327, 345 (2011) ("Additional barriers to the uptake of [genetic cancer risk assessment] services include . . . genetic discrimination, privacy and confidentiality concerns, and fear of the stigma and medical consequences associated with a genetic mutation being identified.").

13. As a two-time breast cancer survivor myself, I am all too familiar with the issues related to genetic testing. In 2004, my oncologist recommended that I be tested to determine if I had either of the two mutations associated with a high risk of breast and ovarian cancer: BRCA1 or BRCA2. As part of the informed consent process, the genetic counselor cautioned me that if I went ahead with testing and my results were positive, it could negatively impact my ability to obtain insurance and affect future decisions by employers. While I had some limited legal protection in Maine under state law, if I moved to a new jurisdiction, it was quite likely that I would be without such safeguards. She explained that this was due to the fact that only a handful of individual states provided substantive protection against genetic discrimination, and at present there was no federal law. Despite the warning, I decided to go ahead with the testing anyway as the information would help inform a number of treatment decisions that I needed to make. Luckily, my results were negative. However, in accord with the similar findings of researchers, I know of numerous women who ultimately declined to forgo such tests out of fear that it might not yield such a favorable outcome, and they would then be without protection for their genetic information.

14. Genetic Information Nondiscrimination Act, Pub. L. No. 110-233, 122 Stat. 881 (2008) (codified at 42 U.S.C. §§ 2000ff to 2000ff-1 (2013)); *see also* OFFICE FOR HUMAN RESEARCH PROT. & DEP'T OF HEALTH AND HUMAN SERVS., GUIDANCE ON THE GENETIC INFO. NONDISCRIMINATION ACT: IMPLICATIONS FOR INVESTIGATORS AND INSTITUTIONAL REVIEW BDS 2 (2009) [hereinafter GINA GUIDANCE], *available at* http://www.hhs.gov/ohrp/policy/gina.pdf. Title I of GINA took effect between May 22, 2009, and May 21, 2010. Title II took effect on November 21, 2009.

related decisions but also the initial acquisition of such data.[15] The original statute had numerous, serious deficiencies due in part to a combination of factors, including GINA's interplay with preexisting laws and the inclusion of several broadly worded exceptions in the statute itself. Further complicating matters was the complete absence of some definitions altogether or the lack of clear and meaningful definitions, which was surprisingly the case with the term "genetic information."

Partially in an attempt to alleviate some of the inadequacies of the Act, the Equal Employment Opportunity Commission (EEOC) proposed and then implemented regulations in 2012.[16] At first glance, the regulations' various additions, clarifications, and modifications appear to improve many of the statute's prior shortcomings. But when examined closely in light of technological advancements in how data is now gathered, stored, and used—as well as the increasing ease with which seemingly anonymized data can be linked to a particular individual—serious deficiencies once again become apparent. These defects threaten the overall goal of GINA and must be corrected to ensure that patients are not deterred from obtaining pertinent healthcare information out of fear regarding how such data might be later utilized.

This Article begins in Part I by discussing in more detail the various technologies that have made it possible to collect, categorize, and retain large quantities of data, as well as the various proposals to regulate such activities. Next, Part II examines whether the concept of non-personally identifiable data truly exists, ultimately concluding that the ability to remain anonymous on the Internet has become, for all intents and purposes, impossible. Part III reviews the provisions of GINA in its current form and the recent regulations promulgated by the EEOC. Part III also provides a comprehensive analysis of the considerable weaknesses of the Act—which are exposed when evaluated in light of the recent technological advancements in data

15. GINA GUIDANCE, *supra* note 14 at 1–2. There are two main titles of GINA, namely Title I, which prohibits the use of genetic information in connection with group health plans, and the aforementioned Title II, which forbids the acquisition and use of genetic information in making decisions with regard to employment. *Id.* A discussion of Title I is beyond the scope of this Article due in part to: (1) the fact that regulations related to this portion of GINA have yet to be finalized, and such regulations are to be promulgated by the Departments of Health and Human Services, Labor, and the Treasury (as opposed to the EEOC, which is responsible for Title II); and (2) questions regarding the way in which it will be interpreted in light of the Patient Protection and Affordable Care Act of 2010.

16. 29 C.F.R. § 1635 (2013). The EEOC was charged with the promulgation of regulations concerning Title II of GINA due in part to GINA's similarity to Title VII of the Civil Rights Act of 1964.

gathering—and proposes model language to eliminate the current gaps in protection. Such changes are imperative to alleviate patients' fears over obtaining genetic testing today due to their concerns regarding the use of their genetic information tomorrow.

I. MONITORING TECHNOLOGY

The Internet has had a dramatic impact on the daily life of most individuals. It has changed the way we interact with one another, conduct business transactions, and access various forms of entertainment. It has also revolutionized the way we acquire knowledge because information on virtually any topic can now be obtained instantly with only a few keystrokes. But what most Internet users are often surprised to learn is the astonishing extent to which our activities on the Internet provide information to a multitude of others. Nowadays, practically "[e]very search, query, click, page view, and link [is] logged, retained, analyzed, and used."[17]

A. Electronic Building Blocks of Online Monitoring

Such pervasive monitoring is accomplished through the use of very small computer files known as cookies, Flash cookies, and beacons.[18] These electronic data gathering programs are unsuspectingly placed on an individual's computer when they visit an Internet site or download free software.[19] According to an in-depth investigation conducted by *The Wall Street Journal* that reviewed one thousand of the most popular websites, tracking technology was found on the vast majority of the sites examined.[20] In fact, in some instances more than 100 monitoring tools were installed as a result of a single visit to a particular site.[21] The website Dictionary.com, for example, exposed users to what the study's authors described as "potentially aggressive surveillance" by installing 168 tracking tools.[22] Of special concern, most of these electronic devices retained the option of collecting health data in light of the statements contained within their privacy policies.[23]

17. Omer Tene & Jules Polonetsky, *To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising*, 13 MINN. J.L. SCI. & TECH. 281, 282 (2012).

18. Angwin, *supra* note 1.

19. *Id.*

20. *Id.*

21. Julia Angwin & Tom McGinty, *Personal Details Exposed Via Biggest U.S. Websites*, WALL ST. J., July 31, 2010, at A1.

22. *Id.*

23. *Id.*

Normally, tracking companies have paid the site's owner for the right to install such files on the computers of those who visit the website.[24] However, it is not uncommon for a site's owner to be unaware of the extent to which large numbers of programs are being downloaded onto a website visitor's computer or, in some circumstances, that such files are even being installed in the first place. But these online tracking tools are merely the basis upon which a virtually unregulated, "emerging industry of data-gatherers[,] who are in effect establishing a new business model for the Internet" has emerged[25]—"one based on intensive surveillance of people to sell data about, and predictions of, their interests and activities, in real time."[26] Furthermore, such electronic monitoring files provide the foundation for an estimated $23 billion online advertising industry.[27]

1. "Ordinary" Cookies

Standard cookies have been around for quite some time and are probably the most well known of the tracking tools. They are small text files, which not only can be innocuous but actually potentially useful to an Internet user.[28] Such programs essentially act as an "identification tag" for a particular computer, thus allowing a website's storage of such simple things as an Internet user's log-in name or possibly a password at the election of the individual.[29] Consequently, users will not be required to reenter this information on each visit to a given website.[30]

However, standard cookies can also be utilized in ways that are arguably quite troublesome. This same technology can also be employed not to merely assist the website visitor but to instead

24. Angwin, *supra* note 1.

25. Angwin & McGinty, *supra* note 21.

26. *Id.*

27. Jennifer Valentino-DeVries & Emily Steel, *"Cookies" Cause Bitter Backlash: Spate of Lawsuits Shows User Discomfort with Latest Innovations in Online-Tracking Technology*, WALL ST. J., Sept. 20, 2010, at B1.

28. *See* Tene & Polonetsky, *supra* note 17, at 289 ("Starting in the 1990s, cookies were initially used to carry information between different web pages and offer re-identification of repeat visitors for usability reasons."); Nick Wingfield, *Microsoft Quashed Effort to Boost Online Privacy*, WALL ST. J., Aug. 2, 2010, at A1 ("Some cookies, such as those installed when a user asks a favorite website to remember his password, don't do tracking.").

29. *See* Wingfield, *supra* note 28; *see also* Interview by Terry Gross, Fresh Air, Nat'l Pub. Radio, with Julia Angwin, Senior Tech. Editor, Wall St. J. [hereinafter Fresh Air].

30. Valentino-DeVries & Steel, *supra* note 27.

benefit third parties generally unknown to the computer user.[31] This is because these text files can alternatively be programmed in such a way that they continuously track Internet users across the entire Web, thereby constructing a vast database of information on an individual's browsing habits and personal interests.[32] The information is then assembled into exceptionally detailed profiles and can often include personal health data.[33]

2. "Special" Cookies

Another category of electronic monitoring tools are those known as "Flash cookies" or "Flash local shared objects."[34] These files are so named because they are installed on an Internet user's computer when an individual visits a website that utilizes Adobe's Flash video player technology.[35] Flash cookies were originally designed to simply store information about a particular user's preferences, such as one's typical volume setting when watching YouTube videos online.[36] However, they can also be used to gather information on a computer user's online browsing activities. In this way, they are functionally similar to ordinary cookies, although Flash cookies have certain attributes that make them potentially even more insidious.[37]

Unlike regular cookies, Flash cookies are stored in an area of a computer that cannot be controlled by a user's Internet browser.[38] Therefore, if an individual takes steps to remove traditional cookies, that process is unlikely to have any impact on these "special" cookies.[39] Consequently, the Flash cookies will still remain and

31. Wingfield, *supra* note 28; Fresh Air, *supra* note 29.

32. Wingfield, *supra* note 28.

33. THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 11 (2012) [hereinafter WHITE HOUSE REPORT].

34. FTC PRELIMINARY REPORT, *supra* note 1, at 66; *see also* Tanzina Vega, *Web Code Offers New Ways to See What Users Do Online*, N.Y. TIMES, Oct. 11, 2010, at A1 (discussing new and future monitoring tools that may be useful in accessing users' online activities but not directly referencing "Flash cookies" or "Flash local shared objects").

35. FTC PRELIMINARY REPORT, *supra* note 1, at 66; Fresh Air, *supra* note 29.

36. Angwin, *supra* note 1.

37. *See* Tene & Polonetsky, *supra* note 17, at 293.

38. FTC PRELIMINARY REPORT, *supra* note 1, at 66 n.154; *see also* Vega, *supra* note 34 (detailing a new type of cookie called an "Evercookie," which stores information in at least ten places on the computer).

39. FTC PRELIMINARY REPORT, *supra* note 1, at 66 n.154. Although not used by the FTC in its report, the phrase "special cookies" has been recognized elsewhere. *E.g.*, Arun Kumar, *Browser Independent*

continue to collect user information. But even more problematic is the fact that the Flash cookies can be used by data collectors to reinstall any of the regular cookies an individual had previously deleted.[40] Such "respawning"[41] can only be prevented if a consumer is knowledgeable regarding the existence of Flash cookies, goes online to Adobe's website, and then successfully follows the instructions supplied to eliminate them.[42]

3. Beacons

A third type of commonly used tracking technology is most often referred to as a "beacon[ ]," although this type is also known as a "Web bug[ ]" or a "pixel[ ]."[43] This tiny piece of computer software runs invisibly on a web page when an Internet user visits a particular site.[44] Beacons can then monitor and record exactly what you are doing while online, such as where your mouse moved or even individual keystrokes.[45]

This category of monitoring tool is unique because instead of being installed on an Internet user's computer, it "run[s] live" while a person is exploring the various pages of a website that contains at

---

Cookies—Lets the Cat Out of the Bag?, THE WINDOWS CLUB (Sept. 4, 2013), http://www.thewindowsclub.com/browser-independent-cookies ("What does a Flash cookie do? Let's take a look at these special cookies, what they do, if they are bad and how to remove them, if need be."); *Flash Cookies and What You Don't Know*, NDARKNESS (Oct. 10, 2009), http://www.ndarkness.com/2009/10/62/flash-cookies-and-what-you-dont-know/ ("The technology I am referring to is the flash plugin, currently developed by Adobe. These 'special' cookies are not created or treated the same way as the cookies that we have all come to know and love. In fact your browser has, on its own, no control over these cookies at all.").

40. Angwin, *supra* note 1.

41. Although not used by Ms. Angwin in her article, the term "respawn" is widely used to refer to a Flash cookie's ability to reinstall regular cookies. *E.g.*, Bose v. Interclick, Inc., No. 10 Civ. 9183(DAB), 2011 WL 4343517, at *1 (S.D.N.Y. Aug. 17, 2011) ("When a computer user deletes a browser cookie, the flash cookie 'respawns' the browser cookie without notice to or consent of the user."); ALEECIA M. MCDONALD & LORRIE FAITH CRANOR, A SURVEY OF THE USE OF ADOBE FLASH LOCAL SHARED OBJECTS TO RESPAWN HTTP COOKIE 3 (2011), *available at* http://www.casos.cs.cmu.edu/publications/papers/CMUCyLab11001.pdf.

42. Angwin, *supra* note 1; FTC PRELIMINARY REPORT, *supra* note 1, at 66 n.154.

43. Angwin, *supra* note 1.

44. *Id.*; *see also Fresh Air*, *supra* note 29 (explaining that the beacon runs in the background while a person navigates a web page).

45. Angwin, *supra* note 1.

least one beacon.[46] Moreover, this is usually the case because a website typically contains multiple beacons from various third parties. In fact, in the earlier discussed study conducted by *The Wall Street Journal*, the majority of websites examined had at least seven beacons from outside companies, including one popular website that had more than forty.[47] Furthermore, many of the identified businesses that perform this electronic monitoring have acknowledged that, among other things, they actually track health conditions.[48]

B. Regulation of Tracking Activities

The legality of online tracking as a whole is quite unsettled. This is due in part to the fact that the legal system has not been able to adequately keep pace with the rapid changes in technology. Consequently, the legal status of placing monitoring programs on Internet users' computers without their consent, as well as the subsequent collection and later use of data that these electronic tools facilitate, is not clear. While these activities arguably implicate statutes such as the federal Computer Fraud and Abuse Act (CFAA), which prohibits accessing a computer without authorization,[49] or possibly federal wiretapping legislation,[50] there are no statutes or regulations directly on point.[51]

1. Lawsuits

The few decisions that have been handed down regarding electronic tracking tools have only considered the legality of ordinary cookies.[52] In 2001 and 2003, two separate federal courts held that advertising companies did not violate federal laws by placing standard cookies on the computers of Internet users who visited websites with

46. *Fresh Air*, *supra* note 29; *see also* Angwin, *supra* note 1 (explaining generally how a beacon tracks a visitor on a website).

47. Angwin, *supra* note 1 (noting that, according to the study, Dictionary.com had forty-one beacons, the most for any site examined).

48. *Id.*

49. Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2006). For a detailed analysis of the CFAA's introductory statement, see Christine S. Davik (f/k/a Christine Davik Galbraith), *ACCESS DENIED: Improper Use of the Computer Fraud and Abuse Act to Control Information on Publicly Accessible Internet Websites*, 63 MD. L. REV. 320 (2004).

50. Electronic Communications Privacy Act, 18 U.S.C. §§ 2510–2522 (2006).

51. *See* Tene & Polonetsky, *supra* note 17, at 313 (stating that, while it is "tangentially subject to various laws, . . . online behavioral tracking remains largely unregulated").

52. Angwin, *supra* note 1; Valentino-DeVries & Steel, *supra* note 27.

which the companies were affiliated.[53] Even so, the precedential impact of these rulings is probably quite limited. This is because the nature of the data gathered and the purposes for which it was then used are arguably rather primitive when compared to the practices of today.[54]

Recently, however, numerous lawsuits have been filed challenging these more powerful, technologically advanced data-gathering programs.[55] The complaints assert that the use of these monitoring devices violates the CFAA and statutes prohibiting deceptive trade practices.[56] Nonetheless, it will likely be some time before any

53. *See* In re Pharmatrak, Inc. Privacy Litig., 329 F.3d 9 (1st Cir. 2003), *dismissed on remand*, 292 F. Supp. 2d 263 (D. Mass. 2003) (holding that while the defendant accidentally collected personally identifiable information, the defendant lacked the requisite intent set forth in the Electronic Communications Privacy Act); In re DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497, 526 (S.D.N.Y. 2001) (holding that tracking did not violate federal law where the trackers only collected information concerning activities on related sites, trackers could not access users' files or programs, and users could easily opt out).

54. *See* Angwin, *supra* note 1 (discussing both the original "basic cookies" and the more advanced "Flash cookies" and "beacons").

55. *E.g.*, Bose v. Interclick, Inc., No. 10 Civ. 9183(DAB), 2011 WL 4343517 (S.D.N.Y. Aug. 17, 2011); *see also* Tene & Polonetsky, *supra* note 17, at 292–94 (stating that numerous class actions have been filed that allege misuse of Flash cookies); Jennifer Valentino-DeVries, *Lawsuit Tackles Files That "Re-Spawn" Tracking Cookies*, WALL ST. J. (July 30, 2010, 7:03 PM), http://blogs.wsj.com/digits/2010/07/30/lawsuit-tackles-files-that-re-spawn-tracking-cookies/ (discussing a lawsuit against Quantcast, ABC, NBC, and others regarding Flash cookies); Valentino-DeVries & Steel, *supra* note 27 (discussing six suits filed in the Central District of California against websites and companies using the more sophisticated tracking software); Tanzina Vega, *Code That Tracks Users' Browsing Prompts Lawsuits*, N.Y. TIMES, Sept. 21, 2010, at B3 (stating that at least five class action suits have been filed against various companies for using Flash cookies).

56. Complaint at 10–14, Rona v. Clearspring Techs., Inc., No. 2:10-cv-07786-GW-JCG (C.D. Cal. Oct. 18, 2010); Complaint at 9–14, Godoy v. Quantcast Corp., No. 2:10-cv-07662-GW-JCG (C.D. Cal. Oct. 13, 2010); Complaint at 59–77, Davis v. VideoEgg, Inc., No. 2:10-cv-07112-GW-JCG (C.D. Cal. Sept. 23, 2010); Complaint at 12–27 Intzekostas v. Fox Entm't Grp., No. 2:10-cv-06586-GW-JCG (C.D. Cal. Sept. 2, 2010); Complaint at 43–57, La Court v. Specific Media, Inc., No. 8:10-cv-01256-GW-JCG (C.D. Cal. Aug. 19, 2010); Complaint at 44–59, White v. Clearspring Techs., Inc., No. 2:10-cv-05948-GW-JCG (C.D. Cal. Aug. 17, 2010); Complaint at 12–19, Aguirre v. Quantcast Corp., No. 2:10-cv-05716-GW-JCG (C.D. Cal. July 30, 2010); Complaint at 99–116, Valdez v. Quantcast Corp., No. 2:10-cv-05484-GW-JCG (C.D. Cal. July 23, 2010); *see also* Tene & Polonetsky, *supra* note 17, at 292 (referring to several of the named cases as bringing claims for the defendants' use of Flash cookies).

significant body of case law emerges regarding the treatment of this new technology.

2. Congressional Measures

The issue of protecting consumers from the pervasive use of monitoring technology is increasingly garnering the attention of Congress. Various legislative proposals[57] have been introduced of late to deal with the public's increasing "discomfort with the tracking of their online searches and browsing activities, which they believe to be private."[58] Congressional bills have generally taken two distinct forms. One category of legislation requires that a consumer be provided with the ability to prohibit entities from gathering and using data about an individual's actions on the Internet, the so-called "Do Not Track" option.[59] The other type is a general privacy statute that would obligate companies to clearly disclose the personal information they collect, reveal how such data is then utilized, and provide consumers with an opt-out mechanism for certain uses.[60]

Currently, however, all of the various bills are stalled in Congress and, not surprisingly, face some significant resistance. Google Inc., Facebook, Apple Inc., and a multitude of other technology-based companies have been vigorously lobbying against congressional proposals that would afford Internet users more control over the ability of companies to monitor their online activities.[61] Reports

57. Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. (2011) (read twice and referred to the S. Comm. on Commerce, Sci., & Transp.); Consumer Privacy Protection Act of 2011, H.R. 1528, 112th Cong. (2011) (referred to the H. Comm. on Energy & Commerce); Best Practices Act, H.R. 611, 112th Cong. (2011) (referred to the H. Comm. on Energy & Commerce); Do Not Track Me Online Act, H.R. 654, 112th Congress (2011) (referred to the H. Comm. on Energy & Commerce); Do Not Track Kids Act of 2011, H.R. 1895, 112th Cong. (2011) (referred to the H. Comm. on Energy & Commerce); Do-Not-Track Online Act of 2011, S. 913, 112th Cong. (2011) (read twice and referred to the S. Comm. on Commerce, Sci., & Transp.).

58. FTC PRELIMINARY REPORT, *supra* note 1, at 20–21.

59. Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1889–90 (2011); *see also* Tene & Polonetsky, *supra* note 17, at 327–32 (detailing the various bills introduced to address consumer privacy concerns).

60. Schwartz & Solove, *supra* note 59, at 1889–90; Jacqui Cheng, *Consumer Groups Skeptical About New Kerry-McCain Privacy Bill*, ARS TECHNICA (Apr. 12, 2011, 4:27 PM), http://arstechnica.com/techpolicy/2011/04/consumer-groups-skeptical-about-new-kerry-mccain-privacy-bill/.

61. Jasmin Melvin, *Web Giants' Consumer Privacy Strategy Faces Hard Sell*, REUTERS (Mar. 10, 2012, 6:59 AM), http://www.reuters.com/article/2012/03/10/internet-privacy-idUSL2E8E5DM520120310.

indicate that industry spending on political activities has soared to $1.2 billion between 1998 and 2011.[62] Furthermore, many of the substantial increases in lobbying expenditures appear to have occurred over the last few years. For example, social media giant Facebook went from spending $351,000 in 2010 to $1.35 million in 2011.[63] Moreover, with continuing congressional gridlock, the probability of passing comprehensive legislation on privacy issues may be low.[64]

3. Administrative Action

The subject of online tracking of Internet users has also become a focus of both the White House and the Federal Trade Commission (FTC). On February 23, 2012, the Obama Administration released a report entitled *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* ("White House Report").[65] Included therein is a "Consumer Privacy Bill of Rights" that, according to the White House, "provides a baseline of clear protections for consumers and greater certainty for businesses."[66] This framework for privacy protection contains seven central principles that ideally should govern the relationship between consumers and businesses.[67] Among them are the rights to "Individual Control," which includes the ability to "exercise control over what personal data companies collect from them and how they use it," and "Respect for Context," which gives

62. *Id.*

63. *Id.*

64. *See, e.g.*, Matthew J. Schwartz, *Do Not Track: 7 Key Facts*, INFORMATIONWEEK (Feb. 24, 2012, 1:10 PM), http://www.informationweek.com/security/privacy/do-not-track-7-key-facts/232601425 (questioning whether the proposed legislation would pass and recognizing that the legislation was built on compromise); *see also* Chris Calabrese, *Time to Get Down to Business on Privacy*, ACLU (Feb. 23, 2012, 12:16 PM), http://www.aclu.org/blog/technology-and-liberty/time-get-down-business-privacy (discussing the White House Report's call for new privacy laws and stating that "the report acknowledges that such legislation isn't imminent").

65. WHITE HOUSE REPORT, *supra* note 33.

66. Press Release, The White House, We Can't Wait: Obama Administration Unveils Blueprint for a "Privacy Bill of Rights" to Protect Consumers Online (Feb. 23, 2012) [hereinafter White House Press Release], *available at* http://www.whitehouse.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights.

67. WHITE HOUSE REPORT, *supra* note 33, at 10 (noting that the seven principles are (1) Individual Control; (2) Transparency; (3) Respect for Context; (4) Security; (5) Access and Accuracy; (6) Focused Collection; and (7) Accountability).

consumers "a 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."[68]

To implement the "Consumer Privacy Bill of Rights," the White House Report recommends a series of discussions with a wide range of various stakeholders to develop enforceable codes of conduct.[69] Additionally, it proposes that there be "greater interoperability between the United States' privacy framework and those of our international partners"[70] and that the FTC be provided with the authority to enforce the Consumer Privacy Bill of Rights.[71] While the White House Report has generally been viewed as a positive step by many privacy and consumer groups, it is merely a framework for substantial, potential objectives.[72] As one major international news agency described it, "[t]he industry got a break last month when the White House released a blueprint 'privacy bill of rights' giving consumers more data control, but relying heavily on voluntary compliance by Internet companies."[73]

A little more than a month after the White House released its report on consumer privacy, the FTC issued its own set of recommendations.[74] The document, *Protecting Consumer Privacy in an Era of Rapid Change*, asserts that it is "intended to articulate best practices for companies that collect and use consumer data" and

68. *Id.* at 11, 15.

69. *Id.* at 2.

70. White House Press Release, *supra* note 66; *see also* WHITE HOUSE REPORT, *supra* note 33, at 31–33 (discussing in detail the need for greater interoperability between the United States' system and international systems and the United States' commitment to creating this interoperability).

71. WHITE HOUSE REPORT, *supra* note 33, at 2.

72. *See, e.g.*, Calabrese, *supra* note 64 (expressing that the ACLU is "gratified that the administration has begun the process" but recognizing that it is a recommendation from which legislation is not imminent); Marcia Hofmann, *Obama Administration Unveils Promising Consumer Privacy Plan, but the Devil Will Be in the Details*, ELEC. FRONTIER FOUND. (Feb. 23, 2012), https://www.eff.org/deeplinks/2012/02/obama-administration-unveils-promising-consumer-privacy-plan-devil-details (applauding the White House's proposal but waiting to see whether these principles will be implemented in a way that effectively protects online privacy).

73. Melvin, *supra* note 61.

74. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012) [hereinafter FTC FINAL REPORT], *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

"assist Congress as it considers privacy legislation."[75] The report calls on companies to give "consumers greater control over . . . their personal data through simplified choices and increased transparency."[76] It recommends that Congress consider enacting "targeted" laws to regulate the practices of data brokers that buy and sell consumer information,[77] as well as to pass baseline privacy legislation.[78]

As with the White House's Consumer Privacy Bill of Rights, these new guidelines issued by the FTC are also only recommendations. Currently, the FTC has taken the position that it does not have the authority to draft new privacy rules, and the report provides that "the framework is not intended to serve as a template for law enforcement actions or regulations under laws currently enforced by the FTC."[79] Consequently, the FTC is dependent on efforts by the industry to self-regulate, which for reasons discussed further in the next section, is problematic.

4. Industry Response

In the wake of increased public attention on the issue of online monitoring tools, advertising and related technology companies began to mount a tenacious campaign against "Do Not Track" initiatives. In 2007, several of the nation's largest trade groups in media, marketing, and advertising joined together to create the Digital Advertising Alliance (DAA).[80] This group, which counts Google, Yahoo!, and Microsoft among its members, was purportedly created to "advocate for responsible advertising behavior by online businesses."[81] However,

75. *Id.* at iii.

76. *Id.* at i.

77. *Id.* at iv.

78. *Id.* at i.

79. *Id.* at vii; Julia Angwin, *Regulators Urge Web Privacy Rules*, WALL ST. J., Mar. 27, 2012, at B3 ("The FTC doesn't have the authority to write new rules for privacy. Instead, it hopes its report will spur the industry to agree to abide by its voluntary guidelines."); *see also* OFFICE OF THE GENERAL COUNSEL, FED. TRADE COMM'N, A BRIEF OVERVIEW OF THE FEDERAL TRADE COMMISSION'S INVESTIGATIVE AND LAW ENFORCEMENT AUTHORITY (2008), http://www.ftc.gov/ogc/brfovrvw.shtm. *But see Federal Trade Commission Calls for Privacy Legislation*, ELEC. PRIVACY INFO. CTR. (Mar. 26, 2012), http://epic.org/2012/03/federal-trade-commission-calls.html (last visited Oct. 15, 2013) (noting that the FTC "fails to explain why it has not used its current Section 5 authority to better safeguard the interests of consumers").

80. Shaylin Clark, *Digital Advertising Alliance Supports Privacy Bill of Rights*, WEBPRONEWS (Feb. 23, 2012), http://www.webpronews.com/daa-supports-privacy-bill-of-rights-2012-02.

81. *Id.*

much of the consortium's work has focused on the creation of industry self-regulatory measures "in an effort to fend off federal regulation."[82]

In July 2009, the DAA issued its report, *Self-Regulatory Principles for Online Behavioral Advertising* ("OBA Principles").[83] This document provides for various standards in the areas of education, transparency, consumer control, data security, changes to existing policies, sensitive data, and accountability. For example, it "instruct[s] members to provide notice, either in an ad or on a Web site . . . that behavioral information is being collected" as opposed to including it among the maze of terms contained within a typical privacy policy.[84] In accordance with the OBA Principles, the DAA also established a program that allows consumers to opt out of targeted advertising.[85] While initially these developments might appear to constitute a significant step forward in protecting consumer privacy online, in actuality they add very little. This is due to the voluntary nature of the assurances, numerous exceptions, and the initiative's especially limited scope.

For example, even when an Internet user exercises an opt-out choice under this DAA initiative, it only requires participating members to cease using electronically gathered data to distribute targeted advertisements.[86] It in no way restricts the ability of companies to continue tracking and collecting information regarding consumers' online activities. Nor does it limit a DAA member's utilization of such data for virtually any other purpose aside from providing customized advertising to Internet users.[87] Thus, even when

82. Stephanie Clifford, *Industry Tightens Its Standards for Tracking Web Surfers*, N.Y. TIMES, July 2, 2009, at B4.

83. *DAA Announces Guidance for Self-Reg Principles in Mobile Environment*, DIGITAL ADVERTISING ALLIANCE, http://www.aboutads.info (last visited Oct. 15, 2013) [hereinafter DAA OBA Principles].

84. Clifford, *supra* note 82.

85. FTC FINAL REPORT, *supra* note 74, at 4; DAA OBA Principles, *supra* note 83.

86. *See* Julia Angwin, *Web Firms to Adopt "No Track" Button*, WALL ST. J., Feb. 23, 2012, at B1 [hereineafter Angwin, *Web Firms*]; Edward Wyatt & Tanzina Vega, *Conflict Over How Open "Do Not Track" Talks Will Be*, N.Y. TIMES, Mar. 30, 2012, at B3; *see also White House, DOC and FTC Commend DAA's Self-Regulatory Program to Protect Consumer Online Privacy*, DIGITAL ADVERTISING ALLIANCE (Feb. 23, 2012), http://www.aboutads.info/resource/download/DAA%20White%20 House%20Event.pdf; Julia Angwin, *Microsoft's "Do Not Track" Move Angers Advertising Industry*, WALL ST. J.: DIGITS (May 31, 2012, 8:09 PM), http://blogs.wsj.com/digits/2012/05/31/microsofts-do-not-track-move-angers-advertising-industry/.

87. Angwin, *Web Firms*, *supra* note 86; Wyatt & Vega, *supra* note 86.

a consumer affirmatively chooses to opt out, the advertising industry can still persist in employing electronic tools to monitor the consumer's online activities.[88]

Two years later, due in significant part to increased pressure from the FTC, the DAA published its *Self-Regulatory Principles for Multi-Site Data* ("Multi-Site Principles").[89] These new standards seemingly extended the very narrow reach of the OBA Principles in two ways. First, the Multi-Site Principles appear to allow consumers to now potentially opt out of the gathering of all data related to their activities online conducted by DAA Members.[90] However, "[w]hile the supplementary principles begin with broad language about collection limits, they incorporate vast exceptions that wholly swallow the rule."[91] For instance, the Multi-Site Principles provide an exemption from the requirement of granting Internet users a choice in whether or not they are electronically monitored for purposes of "market research and product development."[92] As one academic commentator testified in connection with a recent congressional hearing on the subject of online tracking, the exception is "so open-ended that I have not been able to discern any limits on collection . . . [and it] would seem to include keeping track of every click made by a consumer."[93]

88. Angwin, *Web Firms*, *supra* note 86; Wyatt & Vega, *supra* note 86.

89. *Self-Regulatory Principles for Multi-Site Data*, DIGITAL ADVERTISING ALLIANCE (Nov. 2011), http://www.aboutads.info/resource/download/Multi-Site-Data-Principles.pdf [hereinafter DAA Multi-Site Data Principles]. An overview of the report states that the DAA is "[b]uilding on and adopting the recommendations by the FTC in its recent privacy report regarding the collection of Web viewing data." *See About the Self-Regulatory Principles for Multi-Site Data*, DIGITAL ADVERTISING ALLIANCE, http://proxy.chary.us/www.aboutads.info/msdprinciples (last visited Aug. 21, 2013).

90. DAA Multi-Site Data Principles, *supra* note 89, at 1 (noting in the introduction to the report that the "Multi-Site Data Principles extend beyond collection of data for OBA purposes and apply to all data collected from a particular computer or device regarding Web viewing over time and across non-Affiliate Web sites").

91. Jonathan Mayer, *A Brief Overview of the Supplementary DAA Principles*, CTR. FOR INTERNET AND SOCIETY (Nov. 8, 2011, 11:51 PM), http://cyberlaw.stanford.edu/node/6755.

92. DAA Multi-Site Data Principles, *supra* note 89, at 2–3.

93. *The Need for Privacy Protections: Is Industry Self-Regulation Adequate?: Hearing Before the S. Comm. on Commerce, Sci. & Transp.*, 112th Cong. 27 (2012) (statement of Peter Swire, Professor of Law, The Ohio State University). Professor Swire stated further: "My understanding, under the 2011 DAA principles, is that under the market research and product development exceptions: Companies have no transparency requirement; Companies have no consumer choice requirement; Companies can keep the data indefinitely; Companies can identify data that is collection without the user's name, and combine it

The other major change purportedly achieved through the Multi-Site Principles is the prohibition against using data collected for certain categories of potentially problematic purposes. Of particular relevance to this Article is the new proscription on utilizing collected information for "[d]etermining adverse terms and conditions of ineligibility for employment, promotion, reassignment, sanction, or retention as an employee."[94] While heralded by the DAA as a significant restriction, this provision has been criticized for leaving open the option of using such data to instead offer favorable terms or conditions of employment, as well as determine eligibility for a position.[95] Furthermore, a continuing issue with both the standards and recently articulated constraints is the fact that there does not appear to be any substantial consequences for a DAA member that fails to abide by them. As one consumer organization aptly stated: "[T]here are no teeth in the Principles for Multi-Site Data . . . . [T]here are no repercussions spelled out for receiv[ing] a bad report. There's no indication that fines or even formal reprimands will be issued to bad actors, and no provision for removing bad actors from the DAA."[96]

Additionally, a more fundamental problem with the Multi-Site Principles is "why the DAA, as a consortium of organizations in the online advertising space, would have a legitimate claim to regulate third-party web tracking that is not related to advertising."[97] While much attention paid by the public and FTC has been focused on electronic monitoring conducted by Internet advertising and related technology entities, a significant portion of such tracking activity is also undertaken by data brokers, mobile service suppliers, and large

---

with identified data; Companies can combine their data with data from other sources, to build up a more detailed profile; and Companies can share data with other third parties so long as it is not used to market back to the specific computer or device." *Id.*

94. DAA Multi-Site Data Principles, *supra* note 89, at 4. The other categories of prohibited uses are with regard to determining adverse terms and conditions of or ineligibility for credit, health care treatment, or insurance. While the two latter categories may also be relevant in the context of genetic discrimination under Title I as opposed to Title II of GINA, such a discussion is beyond the scope of this paper as stated earlier. *See supra* note 15.

95. Mayer, *supra* note 91 ("The principles do not, however, prohibit offering favorable terms or determining eligibility from third-party web tracking data.").

96. Rainey Reitman, *The DAA's Self-Regulatory Principles Fall Far Short of Do Not Track*, ELEC. FRONTIER FOUND. (Nov. 14, 2011), http://www.eff.org/deeplinks/2011/11/daa-self-regulatory-principles-fall-far-short-do-not-track.

97. Mayer, *supra* note 91.

platform providers, which include Internet Service Providers (ISPs) and social media.[98] Although the FTC is beginning to hold public workshops regarding the impact of data gathering by these additional industry subsets[99] and recommends that Congress pass targeted legislation,[100] it is far from clear whether any non-advertising-based third parties will even agree to adopt the DAA's self-regulatory principles.[101]

Aside from the introduction of self-regulatory principles, the industry has also launched numerous campaigns designed to inform the public about the economic model associated with Internet-based tracking. Many of these public relations efforts highlight the fact that electronic monitoring is arguably a necessary tradeoff for ensuring much of the content on the Internet is available for free because without it, websites would have to start charging users for such information.[102] Other endeavors are much more specific about

98. *See, e.g.*, FTC FINAL REPORT, *supra* note 74, at v.

99. *Id.* With regard to a planned workshop regarding mobile privacy, the report states that staff "will address, among other issues, mobile privacy disclosures and how these disclosures can be short, effective, and accessible to consumers on small screens. The Commission hopes that the workshop will spur further industry self-regulation in this area." *Id.* Additionally, the agency plans to host another workshop focusing on tracking activities by large platform providers. *Id.* ("To the extent that large platforms, such as Internet Service Providers, operating systems, browsers, and social media seek, to comprehensively track consumers' online activities, it raises heightened privacy concerns.").

100. *Id.* The FTC's Final Report on Consumer Privacy recommends the following: "To address the invisibility of, and consumers' lack of control over, data brokers' collection and use of consumer information, the Commission supports targeted legislation—similar to that contained in several of the data security bills introduced in the 112th Congress—that would provide consumers with access to information about them held by a data broker." *Id.*

101. Mayer, *supra* note 91.

102. *See, e.g.*, *How Interest Based Ads Work: Frequently Asked Questions about Online Behavioral Advertising and the Consumer Opt Out Page*, DIGITAL ADVERTISING ALLIANCE, http://www.aboutads.info/how-interest-based-ads-work#about-opt-out (last visited Oct. 16, 2013) ("The most important benefit of online behavioral advertising is the free Internet itself. Many non-subscription websites and online services rely on this type of advertising for revenue, so they do not have to charge users. Every time you check the news or the weather online, scan your favorite gossip site or political blog, or watch a popular TV show or music video on your computer, you are seeing the consumer benefits of online advertising at work."); *see also* Jim Harper, *It's Modern Trade: Web Users Get As Much As They Give*, WALL ST. J., Aug. 7, 2010, at W1 (arguing that consumer tracking is used to sell advertising space, and in return users get free content and further stating that if "Web

particular positive attributes associated with tracking. For example, in January 2012, Google launched "Good to Know," an advertising campaign that included information on how, according to the company, an individual's data makes websites more useful, helps provide relevant search results, and can "even predict disease."[103] This latter benefit refers to Google's "Flu Trends," which monitors search terms entered by the public, and, per the company, these are often "good indicators of actual flu activity" that consequently "provide an early-warning system for outbreaks of influenza."[104] On the surface, this type of health alert service appears exceptionally advantageous and seemingly innocuous. But, as further discussed in Part II, it is made possible in large part by society's increased use of the Internet to obtain health-related information and the simultaneous widespread tracking of these activities.

II. TRACKING, MEDICAL-RELATED INFORMATION, AND LACK OF ANONYMITY

According to a 2011 report published by the non-profit Pew Research Center in Washington, D.C., approximately eighty percent of Internet users go online to obtain health-related information.[105] Additionally, almost twenty percent also utilize the Internet as a means for locating and connecting with other individuals facing similar health issues.[106] But while consumers are acquiring essential medical information and searching for needed support, they risk providing advertisers, marketers, data brokers, and possibly even employers with a host of sensitive information on the Internet users themselves. As the FTC cautioned in its report on protecting consumer privacy online: "The enhanced ability to collect and store consumer data has increased the risks that data will be shared more broadly than understood or intended by consumers or used for purposes not contemplated."[107]

---

users supply less information to the Web, the Web will supply less information to them").

103. *Good to Know*, GOOGLE, http://www.google.com/goodtoknow/ (last visited Aug. 20, 2012) (accessed by searching for the URL in the Internet Archive index).

104. *Good to Know: Data on Google Helping Society*, GOOGLE, http://www.google.com/goodtoknow/data-on-google/helping-society/ (last visited Aug. 20, 2012) (according to Google's website, the company has now also introduced a similar program for dengue fever).

105. Adriana Barton, *Big Pharma Wants to "Friend" You*, GLOBE AND MAIL (July 24, 2011, 4:00 PM), http://www.theglobeandmail.com/life/health-and-fitness/big-pharma-wants-to-friend-you/article4260322/.

106. *Id.*

107. FTC PRELIMINARY REPORT, *supra* note 1, at 21–22.

The scope and breadth of such covert data gathering that can potentially provide information on one's medical-related concerns and conditions is nothing short of astounding. For example, pharmaceutical companies are "using stealth marketing tactics [that include] eavesdropping on patients' discussions on social networks and tracking patients' 'digital footprints' online to target them for advertising."[108] Additionally, other entities—such as search engines, advertising networks, and online social networks—"harvest online conversations and collect personal details from [various Internet sites, including] resume sites and online forums where people might discuss their lives."[109] This enormous amount of data is then used to build detailed profiles of individual behavior over time.[110] According to the FTC, oftentimes these profiles are "broad in scope and large in scale" and may include sensitive information, such as personal medical data.[111] A groundbreaking study by *The Wall Street Journal* showed these individual dossiers often contained "one's age, gender, race, zip code, income, marital status and health concerns, along with recent purchases."[112]

But information brokers contend that these types of data-gathering activities are not unreasonable. The industry maintains that there is nothing improper with their conduct as they are only harvesting material Internet users have chosen to make available. In fact, "[m]any scrapers and data brokers argue that if information is available online, it is fair game, no matter how personal."[113] Furthermore, the industry and its defenders assert that there is a level of personal responsibility associated with these privacy issues. The comments of an essayist in *The Wall Street Journal* are reflective of such views: "[R]ather than indulging the natural reaction to say 'stop,' people should get smart and learn how to control personal information. There are plenty of options and tools people can use to protect privacy—and a certain obligation to use them. Data about you are not 'yours' if you don't do anything to control them."[114] While there may be a modicum of truth to this statement, overall the assessment is quite flawed.

Not surprisingly, recent studies confirm that the vast majority of adults in the United States use the Internet and approximately two-

108. Barton, *supra* note 105.

109. Angwin & Stecklow, *supra* note 7; *see also* WHITE HOUSE REPORT, *supra* note 33, at 11.

110. WHITE HOUSE REPORT, *supra* note 33, at 11.

111. *Id.*

112. Angwin & McGinty, *supra* note 21.

113. *Id.*

114. Harper, *supra* note 102.

thirds have a high-speed broadband connection at home.[115] In today's modern information society, online access is no longer a luxury but is increasingly becoming more of a necessity. Additionally, with such use, inevitably, there is at least some exchange of personal data. But trying to protect this information is not as straightforward as the industry might suggest. This is due in part to the fact that Internet browser developers and computer manufacturers have generally been reluctant to make it easy.

For example, as *The Wall Street Journal*'s Senior Technology Editor Julie Angwin explained in connection with a National Public Radio interview:

> [T]he engineers at Microsoft had a very innovative idea, which was to attempt to block tracking devices from companies that didn't appear to be the one that you were transacting with. So meaning if it's not the website that you're actually visiting and it's some other company installing some tracking device on your Web browser, the default was going to be no, I don't want that. And unfortunately, their view was overruled by the advertising side of the company.[116]

Moreover, even when some sort of privacy protection features are made available to consumers as a possible option, they are often difficult to locate,[117] or the user's choice is ultimately rendered inoperative as some tracking files can be regenerated or circumvented.[118] Consequently, it probably does not come as a surprise that the FTC concluded in its 2012 study on consumer

115. *Internet Use and Home Broadband Connections*, PEW RESEARCH CTR., (July 24, 2012), http://www.pewinternet.org/Infographics/2012/Internet-Use-and-Home-Broadband-Connections.aspx (indicating graphically that approximately eighty percent of adults in the United States use the Internet).

116. *Fresh Air*, *supra* note 29.

117. Wingfield, *supra* note 28 ("Microsoft built its browser so that users must deliberately turn on privacy settings every time they start up the software . . . and those settings aren't always easy to find.").

118. *See, e.g.*, Tene & Polonetsky, *supra* note 17, at 322 ("Even before implementing DNT, most online behavioral tracking companies offer end users the option to opt-out of tracking cookies. Such an opt-out typically relied on the users clicking to accept an opt-out cookie. However, opt-out cookies were often deleted when users cleared their cookie folder, tossing such users unknowingly back into the ad targeting pool."); Angwin, *supra* note 1 ("Some tools surreptitiously re-spawn themselves even after users try to delete them."); Angwin & McGinty, *supra* note 21 (noting that trackers can respawn after users delete them); Valentino-DeVries, *supra* note 55 (claiming certain cookies, per a Berkeley study, "deliberately circumvent controls you set on your computer").

privacy[119] that "many consumers face challenges in understanding the nature and extent of current commercial data practices and how to exercise available choices regarding those practices."[120]

Electronic data gatherers also make one other focal argument in attempting to defend their practices. They contend that tracking is not a violation of consumer privacy because the information collected is not personally identifiable. In other words, since the data sold often does not initially include the actual names of individuals, data gatherers argue that there is no cause for concern.[121] As the following renowned examples illustrate, the force of this claim hinges on a distinction without a difference because advances in technology have made it much easier to turn what arguably may be classified at first as non-personally identifiable information into personally identifiable data.

A. AOL Search Inquiries

In 2006, America Online (AOL) publicly released almost twenty million search queries conducted by more than six hundred thousand of its customers.[122] The raw data sets were placed on a special AOL website that was intended to be utilized by academic researchers studying the online behavior of Internet users.[123] The records included "the date and time of each inquiry and the address of the Web site the user chose to visit after searching."[124] However, obviously personally identifiable information had not been included, such as the actual names or screen names of the customers or their computers' IP addresses.[125] Instead, AOL replaced this data with randomly assigned numbers, and consequently the information was thought to be completely anonymized.[126]

However, a number of reporters from *The New York Times* were able to show that at least part of this information could be

119. *See supra* Part I.B.3 for more information about the FTC's report.

120. FTC FINAL REPORT, *supra* note 74, at 35.

121. Angwin & McGinty, *supra* note 21.

122. Saul Hansell, *AOL Removes Search Data on Vast Group of Web Users*, N.Y. TIMES, Aug. 8, 2006, at C4.

123. Katie Hafner, *Tempting Data, Privacy Concerns: Researchers Yearn to Use AOL Logs, but They Hesitate*, N.Y. TIMES (Aug. 23, 2006), at C1.

124. Hansell, *supra* note 122.

125. Ohm, *supra* note 5, at 1717; Schwartz & Solove, *supra* note 59, at 1818, 1836; Michael Barbaro & Tom Zeller Jr., *A Face Is Exposed for AOL Searcher No. 4417749*, N.Y. TIMES, Aug. 9, 2006, at A1; Hafner, *supra* note 123.

126. Ohm, *supra* note 5, at 1717; Schwartz & Solove, *supra* note 59, at 1818, 1823–24; Barbaro & Zeller, *supra* note 125; Hafner, *supra* note 123; Hansell, *supra* note 122.

reidentified without much difficulty.[127] The article described in detail the way they were able to link various queries, including searchers for "numb fingers," "60 single men," and "dog that urinates on everything" to a sixty-two-year-old woman named Thelma Arnold who lived in Lilburn, Georgia.[128] Ms. Arnold confirmed to a reporter that these inquiries and a host of others were in fact hers.[129]

Her searches, like those of the more than half a million other users included in the AOL database, appear to reveal the concerns, interests, and curiosities of each individual. Nonetheless, while such inquiries may provide "much about the person who typed them, they can also prove highly misleading."[130] For example, Ms. Arnold's quest for information online seemed to indicate that she may be suffering from a wide range of possible physical and mental ailments because her search history also contained queries on "hand tremors," "nicotine effects on the body," "dry mouth," and "bipolar."[131] Such a conclusion would appear to be incorrect, however, as Ms. Arnold admitted in an interview that "she routinely researched medical conditions for her friends to assuage their anxieties."[132] For example, regarding her nicotine inquiries, Ms. Arnold said, "I have a friend who needs to quit smoking and I want to help her do it."[133]

B. Professor Sweeney Study

Dr. Latanya Sweeney conducted a study to illustrate the ease with which supposedly anonymous medical data could be reidentified by combining it with what could be described as fairly ordinary and publicly accessible information—namely voter registration lists.[134] In Massachusetts, an entity called the Group Insurance Commission (GIC) was responsible for procuring health insurance for all individuals employed by the state. In connection therewith, GIC

127. Barbaro & Zeller, *supra* note 125 ("It did not take much investigating to follow that data trail to [a person]."); *see also* Hansell, *supra* note 122 (showing how the information creates composite profiles with all but a name).

128. Barbaro & Zeller, *supra* note 125.

129. *Id.*

130. *Id.*

131. Barbaro & Zeller, *supra* note 125; Hansell, *supra* note 122.

132. Barbaro & Zeller, *supra* note 125.

133. *Id.*

134. *Recommendations to Identify and Combat Privacy Problems in the Commonwealth*: *Hearing on H.R. 351 Before the Pennsylvania House Select Committee on Information Security*, 189th Sess. (Oct. 5, 2005) (statement of Latanya Sweeney, Associate Professor, Carnegie Mellon Univ.), *available at* http://dataprivacylab.org/dataprivacy/talks/Flick-05-10.html#testimony.

gathered detailed patient data for the more than one hundred thousand employees and family members also insured under the policy. GIC eventually decided to release this information to researchers and industry, but before doing so, it expunged all explicit identifiers, including names, addresses, and Social Security numbers. GIC believed these steps would ensure that the data made public was no longer personally identifiable.[135]

Dr. Sweeney purchased the voter registration list for Cambridge, Massachusetts, for a nominal fee—information that is now often available online for immediate download in many jurisdictions. The record provided the name, address, zip code, birth date, and gender for each person. Dr. Sweeney then showed how the two datasets could be combined to reveal the diagnoses, procedures, and medications for named individuals, including the then Massachusetts Governor, William Weld. This was possible because only "six people [on the Cambridge voter list] had his particular birth date; only three of them were men; and, he was the only one in his 5-digit ZIP code."[136] Ultimately, "[i]n a theatrical flourish, Dr. Sweeney sent the Governor's health records (including diagnoses and prescriptions) to his office."[137]

C. The "Fiction" of Non-personally Identifiable Information

As the preceding examples illustrate, people who initially appear to be completely hidden in an anonymous database can often be reidentified.[138] Consequently, "the traditional distinction between [personally identifiable information and supposedly anonymous or de-identified information] has eroded" and "information practices and restrictions that rely on this distinction are losing their relevance."[139] According to an FTC report, "[s]everal factors have contributed to the breakdown of this dichotomy . . . [including] the comprehensive scope of data collection" and the enhanced ability on the part of businesses "to combine disparate bits of 'anonymous' consumer data from numerous different online and offline sources into profiles that can be linked to a specific person."[140]

The question of how best to contend with these developments has generated a vigorous academic debate. Some advocate abandoning the

135. *Id.*

136. *Id.*

137. Ohm, *supra* note 5, at 1720 (citing Henry T. Greeley, *The Uneasy Ethical and Legal Underpinnings of Large-Scale Genomic Biobanks*, 8 ANN. REV. GENOMICS & HUM. GENETICS 343, 352 (2007)).

138. *Id.* at 1703.

139. FTC PRELIMINARY REPORT, *supra* note 1, at 35–36.

140. *Id.* at 36.

concept of non-personally identifiable information altogether. For example, Professor Helen Nissenbaum argues:

> The private/public dichotomy . . . is not useful as the foundation of a normative conception of privacy. Although, in the past, it might have served as a useful approximation for delineating the scope of a right to privacy, its limitations have come to light as digital information technologies radically alter the terms under which others—individuals and private organizations as well as government—have access to us and to information about us in what are traditionally understood as private and public domains.[141]

Similarly, Professor Paul Ohm argues: "[W]e must abandon the pervasively held idea that we can protect privacy by simply removing personally identifiable information (PII). This is now a discredited approach. Even if we continue to follow it in marginal, special cases, we must chart a new course in general."[142] Accordingly, Ohm maintains that the optimal approach to protect privacy is "by squeezing and reducing the flow of information in society, even though in doing so they may need to sacrifice, at least a little, important counter values like innovations, free speech, and security."[143]

Others, however, suggest that the better method is not to abandon the principle of personally identifiable information altogether but possibly to refine it and create a more nuanced approach. Professors David Schwartz and Daniel Solove propose reconceptualizing "a standard for PII" as they anticipate "increasing the benefits from analysis of large data sets in ways we might not be able to predict in advance."[144] As such, they propose three categories of information: "[Information which refers to] an (1) identified, (2) identifiable, or (3) non-identifiable person." Then Schwartz and Solove provide three different regimes of regulation based on traditional Fair Information Practices, noting that "[b]ecause these categories do not have hard boundaries, we define them in terms of standards."[145] According to Professors Schwartz and Solove, if privacy law discarded the concept of personally identifiable information it

141. HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 116–17 (2010).

142. Ohm, *supra* note 5, at 1742.

143. *Id.* at 1706.

144. Schwartz & Solove, *supra* note 59, at 1868, 1871.

145. *Id.* at 1877.

"would be left without a means for establishing coherent boundaries on necessary regulation."[146]

While the answer to which approach to analyzing personally identifiable information is the more salient one is unclear, the idea that there is one singular, comprehensive method for dealing with the problems produced by the increasing ability to reidentify would seem to be incongruous. This appears especially so in light of the fact that "[r]eidentification has arguably taken on special importance in the health privacy context."[147] As such, Professor Ohm's mandate to "reexamine every privacy law, asking whether the power of reidentification and fragility of anonymization have thwarted their original designs"[148] seems particularly prudent with regard to GINA.

III. The Provisions of GINA and Current Regulations

Keeping in mind the previous discussion concerning technological changes in the ability to gather and effectively utilize large quantities of information, we turn to the statutory provisions of GINA and the fairly recently implemented final rules promulgated by the EEOC.[149] As a result of the new regulations, "genetic information" is now broadly defined as information from "an individual's genetic tests . . . the genetic tests of that individual's family members . . . and family medical history" and also includes information about "an individual's [or family member's] request for, or receipt of, genetic services."[150] This means that if, for example, there is a high incidence of breast cancer among women in your family, such data constitutes protected "genetic information," even if you have never personally been diagnosed with breast cancer or been tested to determine if you are a carrier of one of the two known genetic mutations for breast cancer.

Title II proscribes not only the use of genetic information in connection with employment-related decisions[151] but also the mere acquisition of genetic information in most circumstances.[152] GINA states that an employer "may not request, require, or purchase genetic information of an individual or family member of the

146. *Id.* at 1865.

147. Ohm, *supra* note 5, at 1716.

148. *Id.* at 1704.

149. 29 C.F.R. § 1635 (2013).

150. 29 C.F.R. § 1635.3(c)(1)(i–iv).

151. 29 C.F.R. § 1635.4(a) ("It is unlawful for an employer to discriminate against an individual on the basis of the genetic information of the individual in regard to hiring, discharge, compensation, terms, conditions, or privileges of employment.").

152. 29 C.F.R. § 1635.8(a).

individual."[153] The regulations also now further clarify that "request" includes "conducting an Internet search on an individual in a way that is likely to result in a covered entity obtaining genetic information."[154]

The rationale for including a ban on not just utilizing genetic information in connection with employment-related decisions but also on merely acquiring it in the first place is the fact that employment discrimination cases are notoriously difficult to prove.[155] Employees are frequently ignorant that discrimination has even occurred. Consequently, in an attempt to prevent discrimination from possibly happening, GINA prohibits access to genetic information that may be the basis upon which discriminatory action might potentially be taken.[156] As Senator Snowe aptly remarked in connection with the introduction of GINA in the Senate:

> [T]he threat of employment discrimination is very real, and therefore it is essential that we take this information off the table, so to speak, before the use of this information becomes more widespread. While Congress has not yet debated this specific type of employment discrimination, we have a great

153. *Id.*

154. *Id.* For example, if a potential employer performed a search on Google for information on me that only included my name ("Christine Davik") or my current academic affiliation ("Christine Davik" and "University of Maine School of Law"), that would not run afoul of the provision, even if the search results listed included "genetic information" as defined by the Act. However, if the search was instead structured to possibly reveal my BRCA1 or BRCA2 status (for example, "Christine" and "Davik" and "BRCA"), to determine if I had a family history of breast cancer (for example, "Christine" and "Davik" and "breast cancer" and "family"), or to ascertain if I was active in an organization that provides support for individuals at an increased risk of hereditary breast cancer due to the existence of the BRCA genetic mutation (for example, "Christine" and "Davik" and "facingourrisk.org"), this could constitute a prohibited act under GINA.

155. *See, e.g.*, EQUAL EMP'T OPPORTUNITY COMM'N, EEOC COMPLIANCE MANUAL ON RACE AND COLOR DISCRIMINATION, 15–13 (Apr. 19, 2006), *available at* http://www.eeoc.gov/policy/docs/race-color.pdf ("Because discrimination often is subtle, and there rarely is a 'smoking gun,' determining whether race played a role in the decisionmaking requires examination of all of the surrounding facts and circumstances." (citing Aman v. Cort Furniture Rental Corp., 85 F.3d 1074, 1081–82 (3d Cir. 1996) ("It has become easier to coat various forms of discrimination with the appearance of propriety, or to ascribe some other less odious intention to what is in reality discriminatory behavior. In other words, while discriminatory conduct persists, violators have learned not to leave the proverbial 'smoking gun' behind.")).

156. 29 C.F.R. § 1635.1(a)(1).

> deal of employment case law and legislative history on which to build.[157]

At first glance, these updated and seemingly expanded definitions appear to give considerably more protection to employees. However, as discussed in greater detail in the next section, a number of the exceptions in the Act nonetheless appear to swallow up much of the potential safeguards wrought by the latest changes. This is particularly so when assessed concurrently with the advancements in electronic data gathering and aggregation.

A. The "Publicly Available Information" Exception

The general prohibition against requesting, requiring, or purchasing genetic information under GINA does not apply when an employer obtains such information from materials that are "commercially and publicly available."[158] However, this "safe harbor" does not exist when the employer "sought access to those sources *with the intent* of obtaining genetic information."[159] Therefore, under the Act as currently drafted, if an employer conducted a preemployment background check and obtained genetic information from a data aggregation service provider, or alternatively by performing his or her own Internet search, this would not run afoul of GINA so long as there was no evidence that the specific goal of such an inquiry was to acquire genetic information. While in the past the likelihood that an employer would even be able to obtain materials that could possibly shed light on a current or potential employee's genetic status was quite low, today such a risk is far from merely theoretical.

Recent studies show that anywhere from approximately twenty percent to a whopping ninety-one percent of employers now rely on social media in one way or another to screen potential job applicants.[160] Of those hiring managers that do utilize such resources,

---

157. 153 CONG. REC. S828, 847 (daily ed. Jan. 22, 2007) (statement of Sen. Olympia Snowe), *available at* http://www.gpo.gov/fdsys/pkg/CREC-2007-01-22/pdf/CREC-2007-01-22-pt1-PgS828-3.pdf#page=19.

158. 29 C.F.R. § 1635.8(b)(4).

159. 29 C.F.R. § 1635.8(b)(4)(iii) (emphasis added).

160. *See* Steve Johnson, *Like or Dislike? Employers Are Increasingly Screening Applicants Through Online Profiles*, SAN MATEO CNTY. TIMES, Jan. 17, 2012, at A1 ("Other surveys have found that anywhere from 18 percent to 63 percent of employers review social media sites to assess job candidates."); *Thirty-Seven Percent of Companies Use Social Networks to Research Potential Job Candidates, According to New CareerBuilder Survey*, PR NEWSWIRE, Apr. 18, 2012, http://www.prnewswire.com/news-releases/thirty-seven-percent-of-companies-use-social-networks-to-research-potential-job-candidates-according-to-new-careerbuilder-survey-147885445.html [hereinafter *Other Surveys*] (noting that a new survey from CareerBuilder shows that "[n]early two in five

more than half do so to determine "if the candidate is a good fit for the company culture," and more than a third report that social media assists them with ascertaining whether "the candidate is well rounded."[161] Consequently, the marketplace has rapidly responded to the demand for comprehensive data about prospective or current employees with new companies, products, and services to meet this need. The fact that electronic information gathering has become less expensive and more achievable has undoubtedly facilitated the growth of this new industry.

For example, a company by the name of ISO provides a "Web Presence Search" that it claims makes "it easier to probe the Internet for hard-to-find information on persons of interest."[162] This is purportedly accomplished in part by identifying "an individual's 'web footprint'—the trail of digital information left behind from participation and postings on social networking and other websites."[163] Furthermore, ISO asserts that it then combines "online search results with public record findings from third-party sources, such as data aggregators and government agencies," thereby providing "one of the most effective, innovative ways to compile a comprehensive, multidimensional profile" of a particular individual.[164]

Another firm, Sterling Infosystems, Inc., markets itself as the "leading provider of employment-related background screenings."[165]

---

companies (37 percent) use social networking sites to research job candidates," and "[e]leven percent report they do not currently use social media to screen, but plan to start."); *Job Screening with Social Networks*, REPPLER (Sept. 2011), http://reppler.files.wordpress.com/2011/09/reppler-infographic-job-screening-with-social-networks2.jpg (detailing a survey of 300 hiring professionals showing that ninety-one percent of them use social networking sites to screen prospective employees).

161. *Other Surveys*, *supra* note 160.

162. *New Search Helps Locate Self-reported Social Media Postings*, ISO, http://www.iso.com/Newsletters/ClaimSearch/New-search-helps-locate-self-reported-social-media-postings.html (last visited Oct. 13, 2013) [hereinafter *New Search*].

163. *Web Presence Search*, ISO, http://www.iso.com/Products/ISO-ClaimSearch-Decision-Net/Web-Presence-Search.html#.UjNU19vD_IU (last visited Sept. 13, 2013).

164. *New Search*, *supra* note 162.

165. *Background Screening*, STERLING INFOSYSTEMS (June 30, 2013, 9:57 AM), http://web.archive.org/web/20120630095719/http://www.sterlinginfosystems.com/productsandservices/backgroundscreening (accessed by searching for sterlinginfosystems in the Internet Archive index). For the current website, see *Background Check Solutions for All Industries*, STERLING INFOSYSTEMS (July 22, 2010), http://www.sterlinginfosystems.com/sterling-infosystems-acquires-screening-international.htm (stating that "Sterling Infosystems, Inc. [is] a leading provider of employment and background services").

Sterling also claims it provides "the business intelligence companies need to help select the highest quality employees" and "delivers pre-employment background checks that satisfy the specific needs and rigorous standards of any employer."[166] Through its Tandem Select Company, Sterling offers a "Social Intelligence Hiring" service to "human resources, legal, compliance, and risk management professionals."[167] These social media background-search-report products supposedly "facilitate better hiring decisions and reduc[e] organizational risk" by screening potential employees and monitoring current employees.[168] According to the company's website, its products and services are purportedly "legally defensible" and "usable in the hiring process" as reports redact "protected class and other information not relevant to the position."[169]

Even with claims that a company affirmatively screens out "genetic information" (for example, Candidate *A* is BRCA1 positive based on a Facebook post), in the final report sent to the potential employer, the fact that Candidate *A* has searched online for information related to BRCA testing, has "liked" the Facing Our Risk of Cancer Empowered (FORCE) Facebook page—"a nonprofit organization dedicated to improving the lives of individuals affected by hereditary breast and ovarian cancer"[170]—and has participated in numerous five-kilometer races in her community designed to raise money for hereditary breast cancer research, may not be removed. Nonetheless, such data may provide a potential employer with

166. *Background Screening*, STERLING INFOSYSTEMS (June 30, 2013, 9:57 AM), http://web.archive.org/web/20120630095719/http://www.sterlinginfosystems.com/productsandservices/backgroundscreening (accessed by searching for sterlinginfosystems in the Internet Archive index). For the current website, see *Background Check Solution for All Industries*, STERLING INFOSYSTEMS, http://www.sterlinginfosystems.com/other-industry-solutions.htm (last visited Sept. 22, 2013) ("Sterling provides the business intelligence you need to select the highest-quality employees.").

167. *Social Media Background Check*, TANDEM SELECT (Dec. 5, 2011, 12:05 PM), http://web.archive.org/web/20111205120517/http://tandemselect.com/criminal-records-checks/social-media-check (accessed by searching for TANDEM SELECT in the Internet Archive index).

168. *Id.*

169. *Id.* The website additionally states that it generates "FCRA, EEOC, and state law compliant reports based on employer-defined criteria that preserve fair and consistent hiring practices." *Id.*

170. *FORCE: Facing Our Risk of Cancer Empowered*, FACEBOOK, https://www.facebook.com/facingourrisk?fref=ts (last visited Oct. 16, 2013); *see also FORCE: Facing Our Risk of Cancer Empowered*, FACINGOURRISK.ORG, http://www.facingourrisk.org (last visited Oct. 16, 2013) ("FORCE is the only national nonprofit organization devoted to hereditary breast and ovarian cancer.").

substantial clues as to the fact that this individual has probably tested positive for a known genetic mutation or is at a much higher than normal risk for carrying a genetic mutation due to family medical history.

Recently, the FTC has had two separate occasions to examine the legality of these new, expanded forms of background screening and employee monitoring. In May 2011, the FTC gave its tacit approval to Social Intelligence Corporation's Internet and social media screening reports when it completed its investigation of the company and "determined that no further action is warranted at this time."[171] However, the FTC's inquiry into the company was primarily limited to whether Social Intelligence was in compliance with the Fair Credit Reporting Act (FCRA). The FTC concluded that Social Intelligence was in fact a "consumer reporting agency" and as such was required to "take reasonable steps to ensure the maximum possible accuracy of the information reported."[172] Additionally, "[c]onsumer reporting agencies must also provide employers who use their consumer reports with information about their obligations under the FCRA," including the employer's "obligation to provide employees or applicants with notice of any adverse action taken on the basis of these reports."[173] According to Social Intelligence's website, the company "searches millions of websites, including the most well-known social networking websites."[174] Social Intelligence even claims to possess its own "proprietary technology for linking people with pseudonyms or online names they might use in place of the offline name known to their [prospective or current] employer."[175] In response to a request from a reporter, Social Intelligence provided some samples of actual reports provided to employers,[176] including one applicant "whose Internet footprint indicated drug use" as evidenced in part by his participation

171. Letter from Maneesha Mithal, Assoc. Dir., FTC Div. of Privacy and Identity Prot., to Renee Jackson, Member, Nixon Peabody, LLP (May 9, 2011), *available at* http://www.ftc.gov/os/closings/110509socialintelligenceletter.pdf.

172. *Id.*

173. *Id.*

174. *Frequently Asked Questions*, SOCIAL INTELLIGENCE, http://www.socialintel.com/faqs/#emp-1(last visited Sept. 13, 2013).

175. Kashmir Hill, *Feds Okay Start-up That Monitors Employees' Internet and Social Media Footprints*, FORBES (June 15, 2011, 3:34 PM), http://www.forbes.com/sites/kashmirhill/2011/06/15/start-up-that-monitors-employees-internet-and-social-media-footprints-gets-gov-approval/.

176. *Id.* The reporter posted screen shots of the redacted Social Intelligence report. *See, e.g.*, *Social Media Consumer Report*, FORBES BLOG (June 15, 2011), http://blogs-images.forbes.com/kashmirhill/files/2011/06/druggie-applicant.png.

in the Oregon Cannabis Tax Act of 2012 campaign, a citizen's initiative to regulate marijuana and restore hemp "for fuel, fiber and food."[177]

In 2012, the FTC announced that it had settled charges with Spokeo, Inc. in the amount of $800,000.[178] According to the FTC, the company collects personal information on millions of individuals "from hundreds of online and offline data sources."[179] It then "merges the data to create detailed personal profiles," which can include one's hobbies, photos, and participation on social networking sites.[180] The FTC alleged that Spokeo marketed these profiles to human resource professionals, job recruiters, and others in connection with its advertising campaign entitled "Explore Beyond the Resume," which encouraged the use of such reports as an employment screening tool.[181] Additionally, the FTC alleged that Spokeo did not "use reasonable procedures to assure maximum possible accuracy of consumer report information" and also failed to tell employers about their obligation under the FCRA to notify potential or current employees if any adverse action was taken against the individual based on data contained within the report.[182] As with Social Intelligence Corporation, the focus of the FTC's inquiry was largely with regard to potential violations of the FCRA,[183] without any discussion on the general propriety of creating and selling such tools.

While the FTC investigations make clear that entities providing these modern-day background searches must comply with the FCRA, these protections are unsurprisingly insufficient in the context of the

177. *Measure 80—Oregon Cannabis Tax Act of 2012*, PACIFIC GREEN PARTY, http://www.pacificgreens.org/node/47841 (last visited Sept. 13, 2013) (describing the proposed legislation, including the organization's endorsement of the initiative and involvement in collecting over 165,000 signatures to qualify the petition to be placed on the 2012 ballot).

178. *Spokeo to Pay $800,000 to Settle FTC Charges Company Allegedly Marketed Information to Employers and Recruiters in Violation of FCRA*, FED. TRADE COMM'N (June 12, 2012), http://www.ftc.gov/opa/2012/06/spokeo.shtm [hereinafter *Spokeo*].

179. *Id.*

180. *Id.*

181. Complaint at 4, United States v. Spokeo, Inc., No. CV12-05001 (C.D. Cal. June 7, 2012), *available at* http://www.ftc.gov/os/caselist/1023163/120612spokeocmpt.pdf.

182. *Id.* at 6–7.

183. The one claim that was not FCRA-related involved allegations that "Spokeo deceptively posted endorsements of their service on news and technology websites and blogs, portraying the endorsements as independent when in reality they were created by Spokeo's own employees" and as such constituted unfair or deceptive acts. *Spokeo*, *supra* note 178.

potential for genetic discrimination. Furthermore, the language in GINA itself is also inadequate. As such, the current regulations need to be amended to ensure that an employer who conducts a background search on her own, or alternatively purchases such profiles from a third party, does not become privy to genetic information or what I would term "genetic status indicators," namely materials that provide a likely indication of an individual's possible or actual genetic status at either the individual or familial level.

Currently, the safe harbor for receipt of genetic information from commercially and publicly available materials applies so long as the employer did not *intend*[184] to obtain the data. However, such a mens rea is unlikely to be present in the context of conducting or ordering an electronic background search. Consequently, section (b)(4)(iii) must be changed to prevent compromising the statute's protections. The language in section (b)(4)(iii) needs to first be amended to remove the intent requirement and instead provide that the "commercially and publicly available"[185] safe harbor is not applicable to genetic information—or materials that provide a likely indication of a potential or current employee's genetic status, whether personal or familial—if obtained through commercially and publicly available sources that are reasonably likely to result in the acquisition of such information. In the case of searches performed by the employer directly, this would mean that sources "such as Web sites and on-line discussion groups that focus on issues" related to "genetic testing of individuals [or] . . . genetic discrimination" must be avoided so as not to run afoul of the Act if genetic information or genetic status indicators are obtained as a result of said search.[186]

Moreover, when employers are utilizing a third party to conduct a background search, the "commercially and publicly available" safe harbor exception should be amended so as to be inapplicable unless an employer takes additional steps to safeguard against the receipt of genetic information or genetic status indicators. This should include a requirement that an employer must affirmatively request that the entity preparing such a profile not provide any "genetic information" as defined by the Act. Additionally, the employer should be obligated to affirmatively request that any information acquired from sources that are reasonably likely to include genetic information or genetic status indicators "such as Web sites and on-line discussion groups

184. 29 C.F.R. § 1635.8(b)(4)(iii) (2013) (emphasis added).

185. *Id.*

186. 29 C.F.R. § 1635.8(b)(4)(iv).

that focus on issues" related to "genetic testing of individuals [or] . . . genetic discrimination" be excluded.[187]

A similar provision of the Act already makes such a request generally necessary in order to fall within the statutory "safe harbor" in connection with an otherwise lawful inquiry for medical information that results in the receipt of genetic information. Section (b)(1)(i)(B) provides that liability will not attach if the following suggested language is utilized when a request for medical data from an individual or health care provider inadvertently leads to such acquisition:

> The Genetic Information Nondiscrimination Act of 2008 (GINA) prohibits employers and other entities covered by GINA Title II from requesting or requiring genetic information of an individual or family member of the individual, except as specifically allowed by this law. To comply with this law, we are asking that you not provide any genetic information when responding to this request for medical information.[188]

The provision also requires that this language be immediately followed by the definition of genetic information to make clear that this includes not only genetic testing the individual has had but also his or her family medical history:

> 'Genetic information' as defined by GINA, includes an individual's family medical history, the results of an individual's or family member's genetic tests, the fact that an individual or an individual's family member sought or received genetic services, and genetic information of a fetus carried by an individual or an individual's family member or an embryo lawfully held by an individual or family member receiving assistive reproductive services.[189]

These suggested alterations to the "commercially and publicly available" safe harbor provision are necessary to accommodate the changes in the current commercial marketplace and availability of new data products. Failure to make such needed modifications leaves a significant gap in coverage. It also undermines the original objectives and concerns that led to the passage of GINA in the first place.

187. 29 C.F.R. § 1635.8(b)(4)(iv); *Genetic Information Discrimination*, U.S. EQUAL EMP'T OPPORTUNITY COMM'N, http://www.eeoc.gov/laws/types/genetic.cfm (last visited Nov. 29, 2013).

188. 29 C.F.R. § 1635.8(b)(1)(i)(B).

189. *Id.*

B. The "Electronic Water Cooler" Exception

Another exception to GINA's ban on an employer obtaining genetic information applies when the acquisition is unintentional. The statute states that "[t]he general prohibition against requesting, requiring or purchasing genetic information does not apply . . . [w]here a covered entity inadvertently requests or requires genetic information of the individual or family member of the individual."[190] This provision is often referred to as the "water cooler" exception as it ensures that no liability attaches where a supervisor or manager learns genetic information about an employee during a casual, face-to-face conversation, including in response to an ordinary question such as: "How are you?"[191]

The new regulations now extend this exemption to social media as well, providing that an employer will not be held legally accountable if a "manager, supervisor, union representative, or employment agency representative inadvertently learns genetic information from a social media platform which he or she was given permission to access by the creator of the profile at issue (e.g., a supervisor and employee are connected on a social networking site and the employee provides family medical history on his page)."[192] As such, if a supervisor and an employee are "friends" on Facebook and the employee posts information about her mother's recent diagnosis of breast cancer, there would be no liability on the part of the employer for acquiring this genetic information. Consequently, to the extent an employee or potential employee does not want an employer to have access to this type of data, the simple solution is to never post such material, or, alternatively, a supervisor should under no circumstances be an online "friend" in the first place.[193] Increasingly, however, it appears this latter option might not be sufficient.

The possibility that employers or potential employers might seek or require access to one's private social media sites is far from purely hypothetical. This is because many employers now expect applicants

190. 29 C.F.R. § 1635.8(b)(1).

191. 29 C.F.R. § 1635.8(b)(1)(ii)(B) (clarifying that if an individual voluntarily gives information to his or her employer when responding to a general question, the employer does not violate this Act, but the employer may not ask direct or probing questions about the individual's or family members' health).

192. 29 C.F.R. § 1635.8(b)(1)(ii)(D).

193. To the extent that a particular social media profile is accessible to all members of the public—that is, no optional privacy controls are utilized by the creator—then the legality of an employer acquiring genetic information from such a site would need to be analyzed with reference to 29 C.F.R. § 1635.8(b)(4)(ii) regarding publicly available materials. *See infra* Part III.A.

to divulge their social media passwords or grant access to their profiles as part of the interview and preemployment screening process for any sites protected with optional privacy controls.[194] One of the first such cases to rise to the public's attention involved the City of Bozeman, Montana. Applicants there were asked to provide information regarding any social networking sites to which they belonged, along with login data and passwords.[195] Specifically, all candidates for employment with the city received a waiver statement in order to conduct background and reference checks, which sought the following: "Please list any and all, current, personal or business Web sites, Web page or memberships on any Internet-based chat rooms, social clubs or forums, to include, but not limited to: Facebook, Google, Yahoo, Youtube.com, MySpace, etc."[196] The City eventually discontinued the practice,[197] but not before routinely utilizing it for approximately three years.[198]

A somewhat similar situation arose in Maryland at the Department of Public Safety and Correctional Services, which also had a policy of requesting social media usernames and passwords from applicants and current employees seeking recertification.[199] A security

194. *See, e.g.*, Manuel Valdes, *Job Seekers Getting Asked for Facebook Passwords*, YAHOO! FINANCE (Mar. 20, 2012, 7:55 AM), http://finance.yahoo.com/news/job-seekers-getting-asked-facebook-080920368.html.

195. *See* Ki Mae Heussner, *Montana City Asks Applicants for Online Passwords*, ABC NEWS (June 19, 2009), http://abcnews.go.com/Technology/JobClub/story?id=7879939&page=1 (discussing privacy concerns associated with requiring applicants to release information about social media usage).

196. *Id.*

197. *See* Kashmir Hill, *Bozeman, Montana Doesn't Want Your Facebook Password*, FORBES (June 22, 2009, 2:17 PM), http://www.forbes.com/sites/kashmirhill/2009/06/22/bozeman-montana-doesnt-want-your-facebook-password-anymore/ ("Public backlash has prompted the city of Bozeman, Montana to abandon plans to ask job applicants for their usernames and passwords. Effective at 12:00 p.m. today, Friday, June 19, 2009, the city of Bozeman permanently ceased the practice of requesting candidates selected for city positions under a provisional job offer to provide usernames and passwords for the candidate's Internet sites.").

198. Heussner, *supra* note 196.

199. Alexis C. Madrigal, *Maryland Agency Stops Asking Interviewees for Facebook Login*, THE ATLANTIC (Feb. 22, 2011, 4:58 PM), http://www.theatlantic.com/technology/archive/2011/02/maryland-agency-stops-asking-interviewees-for-facebook-login/71582/ (stating that Maryland's Department of Public Safety and Correctional Services does ask applicants to provide log-in information for social medial sites); *see also* Letter from the American Civil Liberties Union of Maryland to Secretary Gary D. Maynard, Secretary, Maryland Department of Public Safety and Correctional Services (Jan. 25, 2011) [hereinafter Letter to

guard, who had taken a leave of absence following the death of his mother, was asked for his Facebook log-in and password information so that his profile could be reviewed in connection with a reinstatement interview.[200] While the officer complied with the request, he reportedly did so only because he feared that he might not otherwise be allowed to return to his former position.[201] The American Civil Liberties Union (ACLU) subsequently complained publicly about the incident,[202] and eventually the Department suspended its practice of asking for social media information.[203]

The instances arising in Montana and Maryland are far from mere anomalies. Comparable cases have been identified in New York, Illinois, and Virginia to name just a few.[204] The practices have also drawn the attention of legislators at both the federal and state level. In March 2012, Senators Blumenthal and Schumer requested that the EEOC and the Department of Justice investigate "a new disturbing trend of employers demanding job applicants turn over their user names and passwords for social networking and email websites."[205] This was followed by Senator Blumenthal and Representative Heinrich introducing federal legislation in May of 2012 in both the

---

Maynard], *available at* http://web.archive.org/web/20120608064847/http://privacyblog.littler.com/uploads/file/ACLU%20Letter%20Jan%2025%202011%20Maryland%20Dept%20of%20Corrections.pdf (detailing Officer Collin's experience during his recertification interview).

200. Valdes, *supra* note 195.

201. *Id.*; Lyneka Little, *What If a Would-Be Employer Wanted Access to Your Facebook Wall?*, ABC NEWS (March 10, 2011), http://abcnews.go.com/Business/employer-turns-facebook-friends-hiring/story?id=13088037.

202. Letter to Maynard, *supra* note 200.

203. Madrigal, *supra* note 200.

204. *See, e.g.*, Valdes, *supra* note 195 (chronicling instances of companies and government agencies asking for log-in data and passwords for social media sites from applicants for employment); Lance Whitney, *Teacher's Aide Refuses to Share Facebook Access, Is Suspended*, CNET NEWS (Apr. 2, 2013, 9:54 AM), http://news.cnet.com/8301-1009_3-57408123-83/teachers-aide-refuses-to-share-facebook-access-is-suspended/ (discussing an incident in Michigan in which a teacher's aide was suspended "after reportedly refusing to show a superintendent her Facebook account").

205. Press Release, Blumenthal, Schumer: Employer Demands for Facebook and E-mail Passwords As Precondition for Job Interviews May Be a Violation of Federal Law; Senators Ask Feds to Investigate (Mar. 25, 2012), *available at* http://www.blumenthal.senate.gov/newsroom/press/release/blumenthal-schumer-employer-demands-for-facebook-and-email-passwords-as-precondition-for-job-interviews-may-be-a-violation-of-federal-law-senators-ask-feds-to-investigate.

Senate and the House.[206] The Password Protection Act of 2012 would have "prohibit[ed] employers from compelling or coercing any person to authorize access to a protected computer, and for other purposes."[207] The bills were never passed; instead, they were referred to Committee,[208] where they simply languished.

At the state level, there has been a recent flurry of legislative activity. As of January 2013, five states have laws barring employers from requiring job applicants or current employees to provide passwords, while ten other states have legislation pending.[209] However, these statutes vary widely in terms of the circumstances in which they apply and the degree of protection they provide.[210] Furthermore, despite the newfound surge of interest in enacting protection, at present the vast majority of states do not have this type of legal assistance to which potential hires or existing employees could turn. Consequently, to the extent that any such statutory safeguards exist, at least in the context of genetic information or genetic status indicators on private social media sites, GINA would most likely need to be utilized.

However, it is not entirely clear that GINA would actually provide the necessary safeguards. As previously mentioned, under the current regulations, employers are not held legally accountable for inadvertently obtaining genetic information from an individual's social media site if they were "given permission to access" the profile.[211] In the previously discussed password cases, employers did not surreptitiously obtain the required log-in data without the potential or current employee's knowledge.[212] Instead, in each instance the information was provided directly from the creator itself, albeit with

206. Password Protection Act of 2012, H.R. 5684, 112th Cong. (2012); Password Protection Act of 2012, S. 3074, 112th Cong. (2012).

207. H.R. 5684; S. 3074.

208. *Id.*

209. *See* Donna Ballmen, *Can Your Employer Demand Your Social Media Passwords?*, AOL JOBS (Jan. 30, 2013, 9:50 AM), http://jobs.aol.com/articles/2013/01/30/employer-social-media-passwords/ (indicating that Maryland, Illinois, California, Michigan, and New Jersey have passed legislation banning employers from asking for social media passwords; Delaware bans educational institutions from asking students for social media passwords; California is contemplating future expansion; and Colorado, Massachusetts, Mississippi, Missouri, Nebraska, New Hampshire, New York, Oregon, Texas, and Vermont are considering legislation).

210. *See* Michelle Poore, *A Call for Uncle Sam to Get Big Brother Out of Our Knickers: Protecting Privacy and Freedom of Speech Interests in Social Media Accounts*, 40 N. KY. L. REV. 507, 521–24 (2013).

212. 29 C.F.R. § 1635.8(b)(1)(ii)(D) (2013).

212. *See supra* notes 196–205.

some concern, hesitation, or possibly both. Nonetheless, this could arguably constitute the necessary consent to allow employers to avail themselves of the exemption from liability.

Consequently, the statute needs to be amended to make clear that this exception can be utilized by an employer only when an individual has "voluntarily" provided access in the true sense of the word. Therefore, to the extent that an employer or potential employer requests access to one's personal e-mail message systems, social networking profiles, or similar sites in the context of evaluating the individual for continued employment, initial hire, or any other employment-related decision, this will not constitute being "given permission" for purposes of the Act. It is vitally important that this actual or perceived ambiguity be remedied to ensure the goals of GINA are met—namely, to provide current or prospective employees with the necessary legal assurances that their genetic information, or even genetic status indicators, will not be obtained or used by an employer. Otherwise, individuals may be deterred from acquiring valuable genetic testing due to concerns over the way in which results obtained could be used against them or their relatives.

C. The "Aggregated Data from Voluntary Wellness Programs" Exception

Under certain circumstances, GINA's general prohibition against acquiring genetic information may be exempted where an employer obtains such data in connection with the provision of a voluntary "wellness program."[213] The general objective of these plans is to improve overall health and fitness so as to prevent detrimental and expensive conditions in the future.[214] According to a study conducted by the Bureau of Labor Statistics, "54 percent of full-time public sector employees and 28 percent of private sector employees had access to a wellness program in 2008."[215] In order to combat rising healthcare costs, "employers are increasingly turning to workplace wellness programs that reward employees who engage in healthy behaviors—or, alternatively, penalize those who don't."[216]

213. 29 C.F.R. § 1635.8(b)(2).

214. Shelley Frost, *Employee Fitness & Wellness Programs*, LIVESTRONG (Jan. 26, 2011), http://www.livestrong.com/article/356864-employee-fitness-wellness-programs/ (discussing the benefits and objectives of employer-sponsored wellness plans).

215. *Id.*

216. Sarah Kliff, *Will Workplace Wellness Programs Work?*, WASH. POST'S WONKBLOG (Mar. 13, 2012, 9:47 AM), http://www.washingtonpost.com/blogs/wonkblog/post/will-workplace-wellness-programs-work/2012/03/13/gIQABWUU9R_blog.html (discussing the effectiveness of workplace wellness programs).

For example, the University of Maine System implemented the "RiseUp Wellness Program" last year.[217] Services are provided by a separate health care company, and it is voluntary in the sense that an employee is not required to participate. Nonetheless, if an employee does not take part in the program, the monthly cost of that employee's premium for health insurance coverage increases substantially, making the decision to enroll less of a choice and more obligatory in nature.[218]

An exemption from liability is provided to employers so long as "individually identifiable genetic information . . . is not disclosed to the employer except in aggregate terms."[219] This provision further provides that an employer does not violate the Act "if it receives information that, for reasons outside the control of the [wellness program] provider or the covered entity (such as the small number of participants), makes the genetic information of a particular individual readily identifiable with no effort on the covered entity's part."[220] Part of the problem with this exception is that neither the original legislation nor the regulations provide a definition of "aggregate" data. Therefore, depending on the level of detail and the manner in which the data sets are enumerated, it is quite possible that the information is non-personally identifiable in name only. Additionally, the prohibition on an employer's attempt at reidentification does not contain any further safeguards. On a more theoretical level, such reidentification bans are generally destined for failure because they are so difficult to enforce.[221] As one academic commentator aptly stated: "How do you detect an act of reidentification? Reidentification can happen completely in the shadows."[222]

In order to strengthen the statute and provide employees with an enhanced measure of protection, the exception should be amended to

217. *RiseUp Wellness Program*, UNIV. OF MAINE, http://www.umsriseup.maine.edu/ (last visited Sept. 16, 2013).

218. *Id.*

219. 29 C.F.R. § 1635.8 (b)(2)(i)(D) (2013).

220. *Id.*

221. Ohm, *supra* note 5, at 1758 ("A reidentification ban is sure to fail, however, because it is impossible to enforce.").

222. *Id.* ("[The] problem [with reidentification bans] appears insurmountable, although four forces might help to ameliorate it. First, lawmakers might pair a ban with stricter penalties and better enforcement, for example by declaring reidentification a felony and providing extra money . . . for enforcement. Second, lawmakers can give citizens a private right of action against those who reidentify. Third, lawmakers can mandate software audit trails for those who use anonymized data. Finally, a smaller scale ban, one imposed only on trusted recipients of specific databases—for example, a ban prohibiting government data-miners from reidentifying—may be much easier to enforce.").

require the employer to affirmatively request that the wellness program provider utilize, at minimum, commercially reasonable methods of data aggregation to safeguard the identity of individual participants in wellness programs when reporting aggregate data to the employer. Failure to do so would preclude the employer from falling within this exception. Such a change is essential to ensure employees are not left with the unenviable choice of conceivably providing an employer access to their genetic information in connection with a "voluntary" wellness program or, alternatively, "choosing" not to participate and thereby possibly facing a significant financial burden in the form of increased monthly healthcare premiums in order to maintain the confidentiality of their genetic status, family medical history, or both.

Conclusion

The overarching issues of tracking consumers' online activities, the ease of identification, and the widespread privacy concerns it raises are progressively receiving more attention not only from legal academics but also from the White House, the FTC, and legislatures at both federal and state levels. Nonetheless, at least in the short term, it appears highly unlikely that there will be a comprehensive solution to the challenges associated with such electronic monitoring. In the meantime, the changes articulated in this Article will strengthen and thus improve GINA. In turn, this will hopefully lessen the hesitancy of patients to obtain the medical testing that could benefit them, thus fulfilling the goals of GINA.

SCHOOL OF LAW

CASE WESTERN RESERVE
UNIVERSITY