



SCHOOL OF LAW
CASE WESTERN RESERVE
UNIVERSITY

**Health Matrix: The Journal of Law-
Medicine**

Volume 24 | Issue 1

2015

Privacy vs. Progress: Research Exceptionalism Is Bad Medicine

Suzanne M. Rivera

Follow this and additional works at: <https://scholarlycommons.law.case.edu/healthmatrix>



Part of the [Health Law and Policy Commons](#)

Recommended Citation

Suzanne M. Rivera, *Privacy vs. Progress: Research Exceptionalism Is Bad Medicine*, 24 *Health Matrix* 49 (2014)

Available at: <https://scholarlycommons.law.case.edu/healthmatrix/vol24/iss1/5>

This Symposium is brought to you for free and open access by the Student Journals at Case Western Reserve University School of Law Scholarly Commons. It has been accepted for inclusion in *Health Matrix: The Journal of Law-Medicine* by an authorized administrator of Case Western Reserve University School of Law Scholarly Commons.

PRIVACY VS. PROGRESS: RESEARCH EXCEPTIONALISM IS BAD MEDICINE

Suzanne M. Rivera[†]

ABSTRACT

Attitudes about privacy are changing in non-research settings, but these attitudinal shifts do not seem to be affecting the way regulators and ethicists think about the need to protect people from the risks of harm resulting from use of personal information in research studies (so-called “informational risks”). Increasingly, people routinely share personal information (including health information) online. And yet, a proposal has been made to restrict further the use of existing data, such as electronic medical records, for purposes of scientific research, even when personal identifiers have been removed. The disproportionate focus on “informational” risks in research is a form of research exceptionalism. This practice of treating research risks with greater caution than we treat other risks encountered in daily life is a legacy of past research abuses. Although understandable in historical context, this exceptionalism is harmful when it unreasonably interferes with scientific advances that could improve human health and welfare.

CONTENTS

INTRODUCTION	50
I. CHANGING ATTITUDES ABOUT PRIVACY	52
II. THE PARADOX OF RESEARCH EXCEPTIONALISM	53
III. HISTORICAL ROOTS OF (PRIVACY) PROTECTIONS IN RESEARCH	55
IV. PRIVACY AND USES OF HEALTH INFORMATION	59
V. FUTURE DIRECTIONS FOR RESEARCH POLICY	61
VI. THE CASE FOR PROGRESS	63

[†] Assistant Professor of Bioethics, Case Western Reserve University School of Medicine; B.A., Brown University; M.S.W., University of California, Berkeley; Ph.D., University of Texas at Dallas. The ideas expressed in this article were presented at the “Balancing Privacy, Autonomy, and Scientific Progress” Symposium convened in April 2013 by the Case Western Reserve University Law-Medicine Center. The author acknowledges and thanks Jessica Berg, Nicole Deming, Michael Householder, and Michelle McGowan for their helpful insights and suggestions.

INTRODUCTION

Privacy is not dead. But it does not look anything like your great-grandmother's privacy. In 1890 Samuel Warren and (the future Supreme Court Justice) Louis Brandeis wrote a seminal piece in the Harvard Law Review called "The Right to Privacy."¹ In it they argued that "[i]nstantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the housetops.'"² In their day, the idea of a still photograph ending up in a newspaper felt like a dangerous threat to civilized society. Imagine what they would think of YouTube.

Attitudes change. Eventually, people in the United States (and around the world) adjusted to a new paradigm for journalistic inquiry that included still photography—an advance that, in hindsight, improved reporting by providing more specific information to readers. This was followed by video journalism and then internet journalism, each bringing about a shift in consumers' expectations about where precisely the camera would go and how the images would be delivered. But, in 1890, as people were still getting used to the newly widespread availability of cameras, a kind of privacy panic took hold.³

When it comes to the (re)use of existing records and data for research today, some privacy advocates are caught up in a similar panic. Worried about snooping by unscrupulous researchers or malevolent third-parties, they portray the secondary use of information, such as that contained in electronic medical records (EMR), as "dataveillance."⁴ Their fear is that re-using existing data for research purposes (including the kinds of public information that are "scraped" from Twitter feeds or Facebook posts) will cause harm to study subjects. And their fear remains even when the data are de-identified because of the possibility of re-identification and a worry that such information could be used in a harmful way (such as discrimination) or used to develop commercial products for which the subjects receive no compensation.⁵

-
1. Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).
 2. *Id.* at 195.
 3. Amitai Etzioni, *The Myth of Privacy Invasion*, CHRISTIAN SCI. MONITOR (September 10, 2001), <http://www.csmonitor.com/2001/0910/p9s1-coop.html>.
 4. DAVID LYON, THE ELECTRONIC EYE: THE RISE OF SURVEILLANCE SOCIETY 47 (1994).
 5. Julia Angwin & Steve Stecklow, "Scrapers" Dig Deep for Data on Web, WALL ST. J. (October 11, 2010), <http://online.wsj.com/article/SB10001424052748703358504575544381288117888.html>.

Others, however, are beginning to recognize that the benefits of gathering and analyzing such data outweigh the real and perceived risks to privacy. Some scientists and research advocates argue that data sources such as EMR and health information posted via the internet are invaluable tools for generation of important new scientific knowledge.⁶ Many beneficial research studies can be done by data analysis without ever interacting with a human subject, and much of the information in question already is publicly available.⁷ One example of the social value of such endeavors is that flu outbreaks can now be predicted more quickly and cost effectively by analysis of Twitter feeds⁸ or Google search terms⁹ than by review of hospital charts. This approach to public health monitoring by analysis of social media data sometimes is called “infodemiology.”¹⁰

We are at a crossroads. Although privacy as a concept still exists, the way we treat information about ourselves is in flux. New technologies make large-scale sharing of information both easy and cost-effective. What previously was considered private is now routinely made public via blogs, twitter feeds, YouTube videos, and Facebook status updates. The question I will address in this paper is: since we share information more freely now than ever before in most aspects of everyday life, why not also do so in the pursuit of science?

-
6. See Damon Centola, *Social Media as a Tool in Medicine: Social Media and the Science of Health Behavior*, 127 CIRCULATION: J. AM. HEART ASS'N 2135 (2013); Peter Jensen et al., *Mining Electronic Health Records: Towards Better Research Applications and Clinical Care*, 13 NATURE REVIEWS: GENETICS 395 (2012).
 7. See, e.g., 17 C.F.R. § 160.3(v) (2013); 15 C.F.R. § 772.1 (2013) (defining “publicly available” as “[i]nformation that is generally accessible to the interested public in any form and, therefore, not subject to the [Export Administration Regulations]”); FTC Privacy of Consumer Financial Information, 16 C.F.R. § 313.3(p) (2013); OFFICE OF ATTORNEY GEN., GUIDELINES FOR DOMESTIC FBI OPERATIONS 44 (2008), available at <http://www.justice.gov/ag/readingroom/guidelines.pdf>.
 8. *Using Twitter to Track the Flu: Researchers Find a Better Way to Screen the Tweets*, SCIENCEDAILY (Jan. 24, 2013), <http://www.sciencedaily.com/releases/2013/01/130124163238.htm>.
 9. Gunther Eysenbach, *Infodemiology: Tracking Flu-related Searches on the Web for Syndromic Surveillance*, in AM. MED. INFORMATICS ASS'N SYMPOSIUM PROCEEDINGS 244, 244 (2006).
 10. Gunther Eysenbach, *Infodemiology and Infoveillance: Framework for an Emerging Set of Public Health Informatics Methods to Analyze Search, Communication, and Publication Behavior on the Internet*, J. MED. INTERNET RES. (2009), <http://www.jmir.org/2009/1/e11/>.

I. CHANGING ATTITUDES ABOUT PRIVACY

Numerous scholars have demonstrated that attitudes about privacy are changing.¹¹ We are growing accustomed to sharing information about ourselves that we used to think of as personal. One catalyst for this shift is the Internet, which facilitates broad electronic self-disclosure by users via venues such as RSS feeds, listservs, chat rooms, and blogs. Not all the information circulating in virtual space is health-related, but many people do post their sonograms on Facebook, tweet about their colonoscopies, and upload their medical histories to health advocacy share sites like PatientsLikeMe (PLM),¹² an online patient community designed to promote health-related information sharing. Online health networks like PLM are “revolutionizing the way patients share their health information and personal experiences, learn about health conditions, add to the body of scientific data, and socialize with other patients.”¹³

We share our information in virtual space because it makes us happy or because we are willing to trade privacy for a service we enjoy or from which we derive benefit. Numerous electronic applications are available now for free or at a modest price, which, in exchange for certain personal information, can deliver services and entertainment. For example, you can have real-time traffic updates texted to your smart phone but only if you allow the provider to track your exact location. The permission to allow geographical surveillance, which in other contexts might seem like an invasion of privacy, is given willingly in exchange for a perceived benefit. Similar applications require personal health information to monitor menstrual cycles and predict ovulation, to count calories, and to aid with smoking cessation. When one considers the scale¹⁴ of the

-
11. Chris Hoofnagle et al., How Different Are Young Adults from Older Adults When It Comes to Information Privacy Attitudes & Policies? 3 (Apr. 14 2010) (unpublished manuscript), available at <http://ssrn.com/abstract=1589864>. See Wen-ying Sylvia Chou et al., *Social Media in the United States: Implications for Health Communication*, J. MED. INTERNET RES. (2009), <http://www.jmir.org/2009/4/e48/>; Deborah M. Moscardelli & Richard Devine, *Adolescents' Concern for Privacy When Using the Internet: An Empirical Analysis of Predictors and Relationships with Privacy-Protecting Behaviors*, 35 FAM. AND CONSUMER SCI. RES. J. 232, 234 (2007).
 12. Jeana H. Frost & Michael P. Massagli, *Social Uses of Personal Health Information Within PatientsLikeMe, an Online Patient Community: What Can Happen When Patients Have Access to One Another's Data*, J. MED. INTERNET RES. (2008), <http://www.jmir.org/2008/3/e15/>.
 13. Patricia Sanchez Abril & Anita Cava, *Health Privacy in a Techno-Social World: A Cyber-Patient's Bill of Rights*, 6 NW. J. OF TECH. & INTELL. PROP. 244, 245 (2008).
 14. Estimates are that Facebook alone has over one billion users worldwide. See Vinodu Goel, *Facebook's Stock Soars Amid Rosy Growth Expectations*, N.Y. TIMES (July 25, 2013, 5:32 PM),

voluntary information sharing that takes place every day online, there is no disputing that perceptions are changing about the nature of privacy itself.

These changes should cause us to question whether our fears about research uses of data are out of step with the way people live today. While attitudes about sharing personal data have been evolving in the Internet age, hesitation about using those data for research purposes persists. Changing societal attitudes about privacy in non-research environments do not appear to inform how regulators think about appropriate protections from so-called informational risks in research. This is reflected in the way research activities are governed. The U.S. regulations pertaining to protection of research subjects¹⁵ still treat privacy like a static object frozen in a twentieth century, analog world. And the rules may soon become even more restrictive. Recent proposals put forth by the Office for Human Research Protections,¹⁶ the federal entity responsible for oversight of federally-funded human research projects, would make it harder for scholars working on bona fide studies to use de-identified data sets. The proposal under consideration would ban the use of de-identified study data unless researchers obtain the informed consent of the people from whom the data originally were derived. Practically speaking, this would render impossible the currently accepted practice of sharing or re-using existing study data as long as the personal identifiers have been stripped to protect the identities of the subjects.

Since people routinely disclose information about themselves outside of research in ways that can be shared, copied, and reused (even for commercial purposes), it is worth considering whether our attitudes about the (re)use of data in a research context also ought to change.

II. THE PARADOX OF RESEARCH EXCEPTIONALISM

For several reasons, we treat research differently than the other activities of life. We apply greater caution to oversight of research studies than we do with dangerous or socially stigmatizing occupations, risky recreational activities, or even the hazards of everyday living routinely encountered in economically-depressed neighborhoods. According to

http://bits.blogs.nytimes.com/2013/07/25/facebooks-stock-soars-amid-rosy-growth-expectations/?_r=1.

15. 45 C.F.R. § 46 (2012). *See also Federal Policy for the Protection of Human Subjects* (“*Common Rule*”), U.S. DEP’T OF HEALTH & HUMAN SERVS., <http://www.hhs.gov/ohrp/humansubjects/commonrule/index.html> [hereinafter *Common Rule*].
16. *See generally* Human Subjects Research Protections: Enhancing Protections for Research Subjects and Reducing Burden, Delay, and Ambiguity for Investigators, 76 Fed. Reg. 44512 (July 26, 2011) (to be codified at 21 C.F.R. pts. 50, 56, 45 C.F.R. pts. 46, 160, 164).

Wilson and Hunter, human research is “much more stringently regulated than many other non-research activities that appear to be at least as risky.”¹⁷ Numerous other scholars also have observed this phenomenon of treating research risks with greater caution than we treat other risks encountered in daily life and, in bioethics circles, it is referred to as research exceptionalism.¹⁸

One of the principal reasons for research exceptionalism is an undeniable and tragic history of past research abuses.¹⁹ Without reviewing here the shameful catalogue of unethical studies conducted in the U.S.,²⁰ it should suffice to say that the current regulatory environment is an understandable response to bad behavior. In addition, some ethicists have argued that—even without the context of past abuses—research is, in fact, different from regular, everyday life and deserves to be treated with greater caution.²¹ But it is not at all clear that the difference in context between research and other non-research activities of life affects or makes more relevant the fundamental ethical principles of respect for persons, beneficence, and justice.²²

Research exceptionalism has paradoxical negative consequences. Although it seeks to protect the subjects (and potential subjects) of research, exceptionalism results in a peculiar kind of paternalism that infringes on their individual liberties. Autonomy (the core of “respect for persons”) is widely considered the foundational principle of human research ethics. But paternalistic protectionism actually infringes on autonomy by presuming to know what is best for others and by limiting their choices to reduce risks. In other words, fear about the possibility of harm results in restrictions on research that prevent people from becoming involved in studies they might very well support.

This paradox illuminates a subtle distinction between the narrow concept of autonomy and the broader principle of “respect for persons,”

-
17. James Wilson & David Hunter, *Research Exceptionalism*, 10 AM. J. BIOETHICS 45, 45 (2010).
 18. See Sally Bean, *Beyond Research Exceptionalism: A Call for Process Redesign*, 10 AM. J. BIOETHICS 58, 59 (2010); see also Sven Ove Hansson, *Reversing “Research Exceptionalism,”* 10 AM. J. BIOETHICS 66, 66 (2010).
 19. See *infra* Part IV.
 20. See Henry K. Beecher, *Ethics and Clinical Research*, 274 NEW ENG. J. MED. 1354 (1966) (discussing numerous “unethical or questionable” studies on humans during a ten-year period following the end of World War II); JONATHAN MORENO, *UNDUE RISK: SECRET STATE EXPERIMENTS ON HUMANS* (1999).
 21. See Wilson & Hunter, *supra* note 17.
 22. Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research, 44 Fed. Reg. 23,192, 23,192-97 (April 18, 1979) [hereinafter Belmont Report].

articulated in the enduringly influential Belmont Report,²³ written in 1979 by the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. Although people often use the idea of autonomy interchangeably with Belmont's "Respect for Persons" principle, it is important to note they are not, in fact, synonymous.²⁴ Respect includes the honoring of a person's expressed autonomy. But a researcher ostensibly can respect a person even if the person cannot (e.g. by virtue of incapacity) or does not choose to assert free will. Indeed, Belmont admonishes that researchers must increase protections for those subjects who are least able to assert autonomy. However, that respectful intention can quickly become paternalistic when applied in the form of unsolicited protection. In the language of Belmont, "Some persons are in need of extensive protection, even to the point of excluding them from activities which may harm them. . . ." ²⁵

With regard to privacy, research exceptionalism takes the form of restrictions or prohibitions against research use of any data or materials that could potentially stigmatize the subjects. But the risk of stigma is too blunt an instrument by which to measure the likelihood or magnitude of the potential for harm. Since attitudes about privacy outside of research are evolving, in the sense that the boundaries between what is public and what is private are becoming more fluid, research regulation around the use of data should evolve, too.

It is not logical to regulate the secondary use of existing research data more strictly than iPod apps or Twitter feeds when millions of people share their personal information for non-research purposes every day. Treating research differently is harmful to public health because it slows progress on solving important problems. In this regard, our focus on privacy protection has become a hindrance to scientific progress, which cannot be justified on ethical grounds. We fuss about it disproportionately. And it is not the only value to be considered when determining whether and how to use health-related information for research.

III. HISTORICAL ROOTS OF (PRIVACY) PROTECTIONS IN RESEARCH

Human research is as old as the medical profession itself. Some point to a nutritional experiment on prisoners described in the Bible's Book of

23. *Id.*

24. M. Therese Lysaught, *Respect: Or, How Respect for Persons Became Respect for Autonomy*, 29 J. MED. & PHIL. 665, 675 (2004).

25. Belmont Report, 44 Fed. Reg. at 23,193.

Daniel as the first documented human clinical trial.²⁶ Despite the fact that physicians and scientists have been studying human subjects since at least as early as Hippocrates, documented concerns about the ethics of using humans in research are only perhaps a few hundred years old. According to Jonathan Moreno, the first efforts to limit research on humans did not occur until the 1890s, when antivivisectionists began calling for laws to protect institutionalized children from being used in medical experiments for vaccine development in the U.S. and in Europe.²⁷

Violation of privacy is widely considered one of the anticipated risks of human research. The notion that privacy violations or breaches of confidentiality could represent a risk of harm to research subjects made its international debut in the World Medical Association's Declaration of Helsinki (first adopted in 1964 and revised eight times, most recently in 2008), which says, "Every precaution must be taken to protect the privacy of research subjects and the confidentiality of their personal information and to minimize the impact of the study on their physical, mental and social integrity."²⁸ This concept was codified in U.S. regulations in 1981 with the promulgation of the Common Rule,²⁹ which requires scientists and ethics committees, called Institutional Review Boards (IRBs), to consider potential invasions of privacy and breaches of confidentiality as risks of research participation worthy of consideration, mitigation, and disclosure.

Privacy is strongly related to autonomy, a core principle of bioethics.³⁰ Autonomy also is an important concept in human research ethics.³¹ In 1974 the U.S. Congress formed a commission to develop national standards for human research conducted with public funds.³² The

-
26. *E.g.*, Duncan Neuhauser & Mireya Diaz, *Daniel: Using the Bible to Teach Quality Improvement Methods*, 13 QUALITY & SAFETY HEALTH CARE 153, 153 (2004).
27. Jonathan D. Moreno, *Goodbye to All That: The End of Moderate Protectionism in Human Subjects Research*, 31 HASTINGS CTR. REP. 9, 10 (2001).
28. WORLD MED. ASS'N, WORLD MEDICAL ASSOCIATION DECLARATION OF HELSINKI: ETHICAL PRINCIPLES FOR MEDICAL RESEARCH INVOLVING HUMAN SUBJECTS 3 (1964), *available at* <http://www.wma.net/en/30publications/10policies/b3/17c.pdf>.
29. *See Common Rule*, *supra* note 15.
30. TOM L. BEAUCHAMP & JAMES F. CHILDRESS, PRINCIPLES OF BIOMEDICAL ETHICS 294 (5th ed. 2001).
31. *Id.* at 57.
32. On July 12, 1974, the National Research Act (Pub. L. 93-348) was signed into law, thereby creating the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research.

commission issued its findings, known as *The Belmont Report*, in 1979.³³ The report articulated three fundamental principles for protection of human research subjects: respect for persons (often used interchangeably with autonomy), beneficence, and justice.³⁴ In a research context, the principle of respect for persons means people should be “treated as autonomous agents” in the sense that we honor the individual’s right to self-determination.³⁵ Privacy and autonomy are conceptually inextricable in the sense that the individual is believed to be entitled to control him/herself, including information about him/herself. Autonomy thus extends beyond the corporeal body and outward, into the sphere of reputation. Therefore, a violation of privacy can be seen as a harm to autonomy (even if only a theoretical, dignitary harm).³⁶

People who work in the field of human research ethics are oriented to think primarily about protection from potential harms. This orientation is understandable, because the bioethics subspecialty of applied research ethics was born out of a response to scandalous research violations resulting in harms to human health, welfare, and dignity—all committed in the name of science. Perhaps the most notorious of these was the Public Health Service-supported “Tuskegee Study of Untreated Syphilis in the Negro Male,”³⁷ but it was by no means an isolated incident.³⁸

The historical imperatives that created our modern research ethics tradition shaped a profession that defaults toward mistrust of investigators and fear of injury or other harms to subjects. Previous abuses inform our thinking about what can go wrong in research and influence the development of rules to prevent recurrences. The journalistic investigation by Rebecca Skloot into the circumstances surrounding the unauthorized creation and use of the HeLa cell line³⁹ showed what can happen to the public’s trust in science and scientists when people feel deceived, violated, and exploited. In short, because research abuses have occurred in the past, we have reason to assume they will again in the future, and we tend to approach the evaluation of potential research

33. Belmont Report, 44 Fed. Reg. 23,192, 23,192-97 (April 18, 1979).

34. *Id.*

35. *Id.*

36. Ruth Macklin, *Dignity is a Useless Concept*, 327 BRIT. MED. J. 1419, 1419 (2003).

37. *U.S. Public Health Service Syphilis Study at Tuskegee*, CTR. FOR DISEASE CONTROL AND PREVENTION, <http://www.cdc.gov/tuskegee/timeline.htm> (last updated Sept. 24, 2013) (acknowledging the U.S. Public Health Service’s intentional failure to treat hundreds of black men for syphilis as part of a study conducted from 1932 to 1972).

38. See Beecher, *supra* note 20, at 1354.

39. See generally REBECCA SKLOOT, *THE IMMORTAL LIFE OF HENRIETTA LACKS* (2010).

through the lens of worry—in some cases too much worry. This has resulted in regulations that, unfortunately, have not kept pace with advances in science.

This tendency toward protectionism has been amplified by comorbid fears about new technologies, such as EMR, cloud-based digital storage media, and social networking websites, all of which often are seen—by research regulators and privacy advocates—as potential instruments of harm from both inadvertent disclosures and deliberate attacks.⁴⁰ Although these fears of new technology may be generational, they are no less real.⁴¹ The age cohort making all the legal and regulatory decisions may feel a little queasy about online avatars giving informed consent in SecondLife⁴² and real-time tweets from hospital operating rooms, but, increasingly, the age cohort of potential research subjects takes for granted the ubiquitous connectivity made possible by these technologies.

With specific regard to secondary uses of EMR data for research, the emphasis on privacy protection is a matter of great consternation. Concerns have been raised about the need to protect individual privacy rights in research because electronic storage and transmission of large data sets could be vulnerable to hacking. Put plainly, even encrypted laptops and password-protected databases somehow feel less secure than the metal filing cabinets and bicycle couriers of yore. Of course, electronic file sharing can make a breach of research data potentially more damaging than the theft of a file cabinet; however, the fear that malevolent uses of existing data are more likely in cyberspace is unfounded. We already have rules against misuse of protected health information for research purposes,⁴³ and there is no evidence to suggest these rules are violated any more than, say, the laws that would prevent a scientist from intentionally killing a research subject or stealing money from a laboratory account.⁴⁴ I would argue that our electronic measures for EMR security provide greater protection (through, for example, file encryption and passwords) and audit trails than the paper folders that

40. Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1771 (2010); Arvind Narayanan & Vitaly Shmatikov, *Privacy and Security: Myths and Fallacies of “Personally Identifiable Information,”* 53 COMMS. OF THE ASS’N. FOR COMPUTING MACHINERY 24, 24 (2010).

41. Hoofnagle et al., *supra* note 11, at 3.

42. SecondLife is “a 3D world where everyone you see is a real person and every place you visit is built by people just like you.” SECONDLIFE, <http://www.secondlife.com> (last visited Apr. 17, 2014).

43. Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. pts. 160, 164 (2013).

used to contain medical records. However, like the person who puts her life at greater risk behind the wheel of a car every day but despairs at the thought of an annual airplane flight, we fear that with which we are less familiar. And even if the material harms of a privacy breach never do come to fruition, the recent flap about the National Security Agency's surveillance of civilian emails and phone calls⁴⁵ has fueled concerns that Big Government (or, in the case of EMR data, Big Pharma) might see something about us we would prefer to keep private.

We place a great deal of importance on privacy in this country, not only because it is a fundamental right in the U.S.,⁴⁶ but because it traditionally has been an aspect of human dignity that we value. And because privacy is linked closely with autonomy, violations of privacy are thought to be synonymous or at least morally equivalent to, violations of personal autonomy. In the realm of research, however, this deference to personal autonomy has failed to keep pace with technological and social changes, including the evolution in attitudes about privacy.

IV. PRIVACY AND USES OF HEALTH INFORMATION

The health information contained in EMR is extremely valuable for clinical trials, discovery research, and public health studies, including post-marketing surveillance.⁴⁷ Analyzing this kind of information is such an efficient way to answer scientific questions that some scholars argue EMR data ought to be treated as a public resource.⁴⁸ Further, it has been suggested that scientific analyses of such data, even without

-
45. Charlie Savage, *N.S.A. Often Broke Rules on Privacy, Audit Shows*, N.Y. TIMES (August 16, 2013), available at <http://www.nytimes.com/2013/08/16/us/nsa-often-broke-rules-on-privacy-audit-shows.html>.
46. See *Katz v. United States*, 389 U.S. 507, 510 (1967) (holding that the FBI's secretly recording a payphone conversation constituted an unreasonable search since the defendant had a "reasonable expectation of privacy" protected under the Fourth Amendment); *Griswold v. Connecticut*, 381 U.S. 479, 485 (1965) (holding that Connecticut's criminalization of contraception violated individuals' right to privacy in their marital relationships).
47. Tjeerd-Pieter van Staa et al., *Pragmatic Randomised Trials Using Routine Electronic Health Records: Putting Them to the Test*, BRIT. MED. J., Feb. 7, 2012, at 1. See also Isaac S. Kohane, *Using Electronic Health Records to Drive Discovery in Disease Genomics*, 12 NATURE REVIEWS GENETICS 417 (2011); Sebastian Schneeweiss, *Developments in Post-Marketing Comparative Effectiveness Research*, 82 CLINICAL PHARMACOLOGY & THERAPEUTICS 143 (2007).
48. Isaac S. Kohane & Russ B. Altman, *Health-Information Altruists — A Potentially Critical Resource*, 354 NEW ENG. J. MED. 2074, 2074 (2005). See also Sharona Hoffman & Andy Podgurski, *Balancing Privacy, Autonomy, and Scientific Needs in Electronic Health Records Research*, 65 SMU L. REV. 85 (2012).

consent, might be considered a “fair use,” along the lines of copyright laws that allow for exceptions to traditional protections in circumstances considered meritorious.⁴⁹

The stakes are sufficiently high that alternatives to the traditional privacy paradigm must be considered. As Lawrence Gostin has argued, “[A] complex modern society cannot elevate each person’s interest in privacy above other important societal interests” like “access to healthcare, more equitable distribution of services to vulnerable populations, and higher quality, better research.”⁵⁰

The ethical principle of beneficence compels us to maximize the value of existing clinical data—whether de-identified or used in an identifiable form with IRB permission and all the applicable requirements to preserve confidentiality—for everyone’s benefit. According to Eric Lander, founder of the Harvard MIT Broad Institute, “If we are going to solve cancer, it is going to take a movement of tens of thousands, or hundreds of thousands, of patients willing to contribute information from their cancer genomes toward a common good.”⁵¹

In research, we require voluminous informed consent documents before volunteers can participate in studies.⁵² We also require review by an independent committee when researchers want to collect identifiable information that could be potentially stigmatizing to subjects.⁵³ And the independent committees that evaluate proposed research studies are expected to pay special attention to justifications for collection of genetic information because of concerns that it could be used to discriminate in health insurance, employment, citizenship, and other legal matters.⁵⁴ However, outside of a research context, we increasingly are willing to share information about our health, or even our DNA, for non-scientific purposes.

23andMe is a company that will, for \$99, map your personal genome.⁵⁵ In addition to yielding information about heritable diseases

-
49. Jessica Berg, *A “Fair Use” Exception for Public Health Uses of Medical Information?*, 43 HASTINGS CTR. REP. 13, 13 (2013).
50. Lawrence O. Gostin, *Health Information Privacy*, 80 CORNELL L. REV. 451, 514-15 (1995).
51. Carl Zimmer, *A Family Consents to a Medical Gift, 62 Years Later*, N.Y. TIMES (Aug. 7, 2013), <http://www.nytimes.com/2013/08/08/science/after-decades-of-research-henrietta-lacks-family-is-asked-for-consent.html>.
52. See 45 C.F.R. § 46.117 (2005).
53. 45 C.F.R. § 46.101(b)(2)(i)–(ii) (2005).
54. See OFFICE FOR HUMAN RESEARCH PROTECTIONS, GUIDANCE ON THE GENETIC INFORMATION NONDISCRIMINATION ACT: IMPLICATIONS FOR INVESTIGATORS AND INSTITUTIONAL REVIEW BOARDS (2009), available at <http://www.hhs.gov/ohrp/policy/gina.html>.
55. 23ANDME, <https://www.23andme.com> (last visited Apr. 17, 2014).

(which is, itself, a matter of some controversy),⁵⁶ the service provides an ancestry analysis that allows customers to “[f]ind out if [they] share an ancestor with famous figures such as Marie Antoinette and Thomas Jefferson.”⁵⁷ Similarly, it is now possible to commission so-called “genetic art,” the likes of which you can purchase from a company called DNA-DX, which will take a genetic sample from you and use it to create a “DNA Portrait” for your living room wall.⁵⁸

Leaving home decorating aside, we derive many benefits from sharing our (health) information and allowing our information to be used by others. Consider the way Amazon and Netflix can tailor suggestions for new purchases personally based upon a customer’s previous selections or their friends’ favorites. What these companies are doing with customer data behind the scenes looks and smells like research but, for most users of the service, the trade-off seems like a good deal. Similar benefits accrue to all customers of a pharmacy when information can be compiled about drug-drug interactions or genetic mutations that make one person more likely than another to respond favorably to a prescription. The perks you enjoy while shopping at Amazon can make healthcare safer – but only when clinical data are put to good research uses that benefit us all.

V. FUTURE DIRECTIONS FOR RESEARCH POLICY

In 2011 the U.S. Department of Health and Human Services (DHHS) made an attempt to update the regulations with an eye toward addressing privacy issues.⁵⁹ The Advanced Notice of Proposed Rulemaking (ANPRM) to solicit feedback on proposed changes to the Common Rule shone a spotlight on privacy concerns in research by suggesting that new, additional protections are warranted to govern the use of existing data – even when the information that could identify individual subjects has been removed.⁶⁰ Such a change would represent a dramatic departure from the prevailing view that de-identified data and specimens pose little or no privacy risk because even highly-stigmatizing

56. See Allen Salkin, *When in Doubt, Spit It Out*, N.Y. TIMES (Sept. 14, 2008), <http://www.nytimes.com/2008/09/14/fashion/14spit.html?ref%3Dstyle&r=1&>.

57. *Discover DNA Ancestry and Genetic History with Our DNA Test*, 23ANDME, <https://www.23andme.com/ancestry/deep/#lineages> (last visited Apr. 17, 2014).

58. *The DNA Portrait*, DNA 11, <http://www.dna11.com/> (last visited Apr. 17, 2014).

59. Human Subjects Research Protections: Enhancing Protections for Research Subjects and Reducing Burden, Delay, and Ambiguity for Investigators, 76 Fed. Reg. 44,512 (July 26, 2011) (to be codified at 21 C.F.R. pts. 50 & 56).

60. *Id.*

information would need to be linked (or reasonably link-able) to the subject in order to pose a risk of material harm.

Unfortunately, the proposed changes would move us in the wrong direction. If adopted, they would establish “mandatory standards for data security and information protection whenever data are collected, generated, stored, or used,” and additional rules protecting against the use of de-identified information that is collected or generated as part of a research study.⁶¹ Specifically, the proposed rule would require written consent for the “study of existing data, documents, records and biospecimens to include all secondary research use of identifiable data and biospecimens that have been collected for purposes other than the currently proposed research” and would prohibit un-consented re-use of existing de-identified data if they were “originally collected for research purposes.”⁶²

Surely, the people who wrote the ANPRM are well-intentioned. They are very concerned about autonomy, which –as explained above – often is regarded as the most important of the three principles considered fundamental in human research: Respect for Persons (a.k.a. Autonomy), Beneficence, and Justice.⁶³ But I would suggest that privileging autonomy over the principles of justice and beneficence is an outdated way of thinking about research ethics and can be harmful.

Disqualifying the use of de-identified data originally collected for research purposes unless subjects are re-consented would be a mistake for three reasons. First, it is illogical. How can you obtain consent from people when you do not know their identities? Secondly, not using existing data would require collection of new data, meaning more people than necessary must be studied to answer important questions. This is wasteful (an injustice, with regard to the distribution of limited resources) and unnecessarily exposes more people to the risk of harm (a violation of beneficence). Finally, it seems to ignore common sense. While patients may have no knowledge (outside of the standard HIPAA warning) that their data can be used for research, subjects who previously have consented to participate in research actually know and agreed that their data can be used for science (and presumably would be more agreeable for further study usage).

Such a change in paradigm would be a case of over-emphasizing individual rights at the expense of group wellbeing. EMR data can be used to answer important questions if we can agree on the value of information altruism. Rather than adding new roadblocks to important research that can improve the human condition, we should—as has been argued by Hoffman and others –instead think about EMR data as a

61. *Id.* at 44,516.

62. *Id.* at 44,515, 44,519 (internal citations omitted).

63. Belmont Report, 44 Fed. Reg. 23,192, 23,192-97 (April 18, 1979).

community asset to be used for the common good.⁶⁴ This would require a shift away from regulations designed to protect us from evildoers and toward promotion (with responsible stewardship) of an ethos that values information sharing.

VI. THE CASE FOR PROGRESS

There is a tension between individual liberties –expressed through an emphasis on privacy protection –and collective benefits, or progress. When we concern ourselves primarily with protection of privacy rights, we focus on the individual and the likelihood and magnitude of at least two kinds of potential harms. First, material harms, in the context of EMR data, could theoretically affect someone’s employability, insurability, immigration status, ability to marry, etc. Second, more abstract notions of harm, like the dignitary harm (infringement of autonomy) could be said to come from unauthorized secondary use of EMR data, even when the subject is unaware of it.⁶⁵ There is also the emotional harm that could come from a discovery about which people would rather not know. For example, if a particular group of people were found to be associated with a dangerous or stigmatizing health condition, that information might injure the status of the group and harm an individual’s morale as a member of that group.

On the other side of the scale, you have scientific progress. As I have tried to show, I find the importance of potential benefit here very compelling –benefit to individuals who can receive better health care and benefit to the larger community of people who can enjoy not only better health but also, potentially, more efficient uses of labor, money, and other resources.

Although one could say, on consequentialist grounds, that invading the privacy (violating the autonomy) of a few people can be justified if it improves the health of many more (other) people, I am not making such an argument. Instead, I am saying that we all benefit when we each participate. And, because I believe this view is consistent with the three fundamental ethical principles of human research protection, I want to touch on each and explain why I think they also justify erring on the side of progress.

With regard to Respect for Persons, our paternalistic impulse to protect actually reduces autonomy in the sense that IRBs and others will

64. See Hoffman & Podgurski, *supra* note 48.

65. See Susan M. Shell, *Kant’s Concept of Human Dignity as a Resource for Bioethics*, in HUMAN DIGNITY AND BIOETHICS: ESSAY’S COMMISSIONED BY THE PRESIDENT’S COUNCIL ON BIOETHICS 333, 334 (2008), available at http://bioethics.georgetown.edu/pcbe/reports/human_dignity/human_dignity_and_bioethics.pdf.

actually be forced to reject protocols out of privacy fears when the individuals affected may very well have been willing either to consent or to allow their data and specimens to have been used without consent. There are no provisions under the current regulations for allowing an adult of sound mind to say, “Use this information for whatever research you please and I’m okay with that.”

Although it could be argued that harm to individual dignity may be created by re-using de-identified data without an individual’s knowledge (a violation of the Respect for Persons principle), the principle of Beneficence calls for a utilitarian assessment of that risk in the context of benefits to subjects and society that could be derived from the knowledge to be gained.⁶⁶ And the principle of Justice suggests a shared responsibility to contribute to beneficial knowledge.⁶⁷ Since the principle of Justice in research means equitable distribution of both risks and benefits, the situation we have now is unfair. Everyone benefits from discoveries made by using data about relatively few people. An ethos of information sharing for the common good would be more just.

The disproportionate protection of privacy in research is not warranted because we already share all sorts of information outside of the research environment. Sharing EMR information would benefit everyone through new scientific discoveries. By letting fear shape science policy, we do more harm than good. Failure to use existing data is an opportunity cost. Or, put another way, limiting progress reduces beneficence.

66. Belmont Report, 44 Fed. Reg. 23,192, 23,192-97 (April 18, 1979).

67. *See id.*