RECONSIDERING CONSTITUTIONAL PROTECTION FOR HEALTH INFORMATION PRIVACY

Wendy K. Mariner *

TABLE OF CONTENTS

* Edward R. Utley Professor of Health Law, Boston University School of Public Health, Professor Law, Boston University School of Law.

INTRODUCTION

Would you agree to allow your physician to give the state health department any of the following information about you personally or your children?

- ☐ A contagious disease, such as tuberculosis, gonorrhea, or HIV
- ☐ A chronic disease, such as a cancer, asthma, or lupus
- ☐ Blood sugar levels
- ☐ Prescriptions for controlled substances
- ☐ Immunizations
- ☐ A newborn child's genetic anomaly
- ☐ The cost of medical care
- ☐ The outcome of medical treatment

The answer may be "it depends." Many people may not care at all whether the state has any or all of their medical information.[1] For others, the answer depends on why the state needs specific information and what it does with that information.[2] State health and social service departments routinely collect health information in all these categories from physicians, hospitals, laboratories, and pharmacies pursuant to various state reporting laws.[3] They may also give the information, with or without personal identifiers, to federal and international agencies and private researchers. Few of these laws require individual consent to either the collection or the uses of a person's information. Should consent be required for any of these laws? What health information should be freely accessible to government and what should not?

These questions arise in the context of competing trends in the age of Big Data: the increasing social and commercial value of health information,[4] and rising concerns about the loss of privacy in the

---

1 *See* Sharona Hoffman & Andy Podgurski, *Balancing Privacy, Autonomy, and Scientific Needs in Electronic Health Records Research*, 65 SMU L. REV. 85, 112–14 (2012) (summarizing varying public opinion poll results); *see also Americans Trust Physicians, Not Government, with Medical Info*, AHC MEDIA (Oct. 1, 1997), http://www.ahcmedia.com/articles/35862-americans-trust-physicians-not-government-with-medical-info (finding that two-thirds of poll respondents would prefer that their physicians and not the government, insurance companies, or employers have access to their medical information).

2 *See infra* text accompanying notes 353–55.

3 *See infra* Part II.

4 *See, e.g.*, M. Rose Gasner et al., *Legal and Policy Barriers to Sharing Data Between Public Health Programs in New York City: A Case Study*, 104 AM. J. PUB. HEALTH 993, 996–97 (2014) (encouraging changes in laws to permit identifiable data sharing among health departments, social service programs, health care facilities, and other agencies); Christopher Rees, *Tomorrow's Privacy: Personal Information as Property*, 3 INT'L DATA PRIVACY L. 220, 220–21 (2013); Marianne Kolbasuk McGee, *Health Research Bill Would Alter HIPAA*, GOVINFO

wake of Edward Snowden's revelation of the National Security Agency's ("NSA") bulk data collection.[5] Furthermore, recent U.S. Supreme Court opinions hint that information held by third parties may warrant some Fourth Amendment protection in the rapidly evolving age of cloud computing.[6] Such judicial hints have encouraged critics of the third-party doctrine to argue that the Fourth Amendment does not give government entirely free rein to obtain information about a person simply because the information is in the hands of a third party.[7] The cases may also inspire a reassessment of whether and how other Amendments might protect personal health information.[8]

SECURITY (May 11, 2015), http://www.govinfosecurity.com/health-research-bill-would-alter-hipaa-a-8214/op-1 (describing privacy concerns about a proposed federal bill, that would allow covered entities to use patients' protected health information for research without patient consent). *But see* The White House, Office of the Press Secretary, Fact Sheet: President Obama's Precision Medicine Initiative (Jan. 30, 2015), http://www.whitehouse.gov/the-press-office/2015/01/30/fact-sheet-president-obama-s-precision-medicine-initiative (proposing NIH cancer research program with at least a million volunteers who contribute their medical records, profiles of genes, metabolites, and microorganisms, environmental and lifestyle data, their own patient-generated information, and personal device and sensor data).

5 *See, e.g.*, PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT 142–43 (Jan. 23, 2014) (noting NSA's arguments that bulk data collection allows instantaneous data retrieval, comparison with historical records, and breadth of relationships with contacts); Spencer Ackerman, *Privacy Experts Question Obama's Plan for New Agency to Counter Cyber Threats*, THE GUARDIAN (Feb. 10, 2015), www.theguardian.com/world/2015/feb/10/obama-cyber-threat-agency-privacy; Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, THE GUARDIAN (June 7, 2013), www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data; *Edward Snowden*, THE GUARDIAN, www.theguardian.com/us-news/edward-snowden (last visited Nov. 4, 2015).

6 *See* Los Angeles v. Patel, 135 S. Ct. 2443, 2451 (2015) (finding that a city ordinance requiring hotel operators to maintain hotel guest records for inspection on demand by police facially violates Fourth Amendment "because it fails to provide hotel operators with an opportunity for precompliance review"); Riley v. California, 134 S. Ct. 2473, 2493 (2014) ("Privacy comes at a cost."); United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) ("[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."); *see also* Kyllo v. United States, 533 U.S. 27, 34 (2001) (asking "what limits there are upon this power of technology to shrink the realm of guaranteed privacy" under the Fourth Amendment).

7 *See generally* Alan Butler, *Get a Warrant: The Supreme Court's New Course for Digital Privacy Rights After* Riley v. California, 10 DUKE J. CONST. L. & PUB. POL'Y 83 (2015) (describing *Riley*'s possible effect on future Supreme Court Fourth Amendment decisions involving new technologies).

8 For analyses of First Amendment implications, see generally ANITA L. ALLEN, UNPOPULAR PRIVACY: WHAT MUST WE HIDE (2011); Anita L. Allen, *First Amendment Privacy and the Battle for Progressively Liberal Change*, 14 J. CONST. L. 885 (2012); Ronald J. Krotoszynski, Jr.,

This Article encourages that reassessment. Part I describes the types of questions that deserve fresh constitutional analysis. Part II summarizes a variety of purposes for which health information is being collected and used today. Part III analyzes the third-party doctrine exception to the application of the Fourth Amendment, which permits the government to obtain information from a third party without the data subject's consent. It concludes that, when closely analyzed, the relevant third-party doctrine cases do not offer useful precedents for evaluating mandatory reporting laws. The administrative search exception and the special needs exception to the Fourth Amendment's requirement of probable cause or individualized suspicion are examined in Parts IV and V, respectively. Like the third-party doctrine examples, these cases offer limited guidance for determining whether government has the power to enact the range of mandatory reporting laws contemplated for contemporary civil purposes. Part VI analyzes Fifth and Fourteenth Amendment protection of health information privacy as an aspect of liberty protected by the Due Process Clause, again finding only partially applicable precedent.

Three conclusions are drawn from this review. The first is that traditional interpretations offer meager constitutional protection for health information privacy. A second conclusion is that traditional interpretations of constitutional doctrine no longer adequately account for either the range of expectations of privacy in health information or the circumstances in which such information should be more or less widely available.[9] Third, as argued in Part VII, there is room for a more sophisticated approach to constitutional protection of health information. Such an approach should recognize current and future dependence on sharing personal information electronically with public and private entities, as well as the dignitary aspect of health information privacy. It should also move from a blanket, bimodal doctrinal model in which the Fourth Amendment, for example, does or does not apply, to a more individualized, purpose-oriented approach, one that increases the level of judicial scrutiny in

---

Reconciling Privacy and Speech in the Era of Big Data: A Comparative Legal Analysis, 56 WM. & MARY L. REV. 1279 (2015).

9 *See* Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326, 378–97 (2015) (describing ways in which uses of data in cyberspace challenge legal doctrines); David G. Delaney, *Widening the Aperture on Fourth Amendment Interests: A Comment on Orin Kerr's* The Fourth Amendment and the Global Internet, 68 STAN. L. REV. ONLINE 9, 12 (May 18, 2015) (arguing that governments should look beyond traditional doctrines derived from law enforcement cases to "to establish suitable search-and-seizure frameworks that match society's dependence on cyberspace").

inverse proportion to the immediacy of the need for the information to respond to existing threats to health or safety.[10]

I. FRAMING THE QUESTIONS

Both the Universal Declaration of Human Rights ("UDHR")[11] and the International Covenant on Civil and Political Rights ("ICCPR")[12] recognize privacy as a human right. Numerous international and regional conventions also contain privacy protections.[13] In December 2013, amid concerns that surveillance adversely affects human rights, the United Nations General Assembly adopted Resolution 68/167 calling on states to protect privacy both offline and online and emphasizing that "international human rights law provides the universal framework against which any interference in individual privacy rights

---

10 For example, Professor Daniel J. Solove recommends abandoning the reasonable expectations of privacy concept in Fourth Amendment doctrine in favor of requiring regulation and oversight "whenever a particular government information gathering activity creates problems of reasonable significance." Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1514 (2010).

11 Adopted and proclaimed by G.A. Res. 217(A) (III) (Dec. 10, 1948) ("Article 12: No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.").

12 Adopted and opened for signature, ratification and accession by G.A. Res. 2200(A) (XXI) (Dec. 16, 1966) ("Article 17: 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks upon his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks."). The United States ratified the ICCPR. United Nations International Covenant on Civil and Political Rights, *opened for signature* Dec. 16, 1966, 999 U.N.T.S. 171 (adopted by the United States June 8, 1992).

13 *See, e.g.*, Comm'n on Human Rights, Status of the International Covenants on Human Rights, U.N. Doc. E/CN.4/1985/4 (Sept. 28, 1984); Vienna Declaration and Programme of Action (1993), U.N. Doc. A/CONF.157/23 (July 12, 1993) (adopted by the World Conference on Human Rights, June 25, 1993); European Convention on Human Rights art. 8, Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 221 ("Everyone has the right to respect for his private and family life, his home and his correspondence."); Treaty of Lisbon: Amending the Treaty on European Union and the Treaty Establishing the European Community art. 16B, Dec. 17, 2007, 2007 O.J. (C 306) 1, 51 ("Everyone has the right to the protection of personal data concerning them."); G.A. Res. 45/158 art. 14, Convention on Migrant Workers (Dec. 18, 1990); G.A. Res. 44/25 art. 16, Convention on the Rights of the Child (Nov. 20, 1989); African Charter on the Rights and Welfare of the Child, Art. 10; American Convention on Human Rights, Art. 11; Declaration of Principles on Freedom of Expression in Africa, Art. 4; American Declaration of the Rights and Duties of Man, Art. 5; Arab Charter on Human Rights, Art. 17; ASEAN Human Rights Declaration, Art. 21; European Convention for the Protection of Human Rights and Fundamental Freedoms, Art. 8; Johannesburg Principles on National Security, Free Expression and Access to Information; Camden Principles on Freedom of Expression and Equality.

must be assessed."[14] Pursuant to the Resolution, the High Commissioner for Human Rights prepared a report on the right to privacy in the digital age.[15] The High Commissioner's Report, *The Right to Privacy in the Digital Age*, was requested primarily in response to anti-terrorism surveillance by the NSA and other nations' security agencies, but its principles are applicable more generally.[16] The High Commissioner noted that digital surveillance practices can negatively affect other human rights, such as the human right to health, "for example where an individual refrains from seeking or communicating sensitive health-related information for fear that his or her anonymity may be compromised."[17] The Report questions "the extent to which consumers are truly aware of what data they are sharing, how and with whom, and to what use they will be put."[18]

The Report summarizes basic principles governing the human right to privacy. First, "surveillance measures must not arbitrarily or unlawfully interfere with an individual's privacy, family, home or correspondence."[19] The Human Rights Committee interprets the prohibition against arbitrary or unlawful measures to mean that even laws that are properly enacted can be "arbitrary" if they contravene provisions, aims or objectives of the ICCPR or are unreasonable in the particular circumstances.[20] More specifically, to be reasonable and not arbitrary, "any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case."[21] To be necessary, an intrusion on privacy must be "the least intrusive option available."[22] These three concepts—legality, necessity, and proportionality—form the core principles of privacy protection in the human rights framework. They can be seen in many in-

14 Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, at para. 5, U.N. Doc. A/HRC/27/37 (June 30, 2014) [hereinafter OHCHR, Right to Privacy]; *see also* G.A. Res. 68/167, The Right to Privacy in the Digital Age (Dec. 18, 2013).

15 G.A. Res. 68/167, *supra* note 14, at 3.

16 OHCHR, Right to Privacy, *supra* note 14, at para. 3. The Report was presented to the U.N. General Assembly on September 14, 2014, and the General Assembly is to follow it up in the future.

17 *Id.* at para. 14.

18 *Id.* at para. 18.

19 *Id.* at para. 15.

20 *Id.* at para. 21; *see also* Human Rights Committee, *General Comment 16* (Twenty-third session, 1988), COMPILATION OF GENERAL COMMENTS AND GENERAL RECOMMENDATIONS ADOPTED BY HUMAN RIGHTS TREATY BODIES, U.N. Doc. HRI/GEN/1/Rev.1 at 21 (1994), http://tbinternet.ohchr.org/_layouts/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=8&DocTypeID=11.

21 OHCHR, Right to Privacy, *supra* note 14, at para. 21.

22 *Id.* at para. 23.

ternational and regional documents, the European Data Directive, and in the various versions of Fair Information Practices principles.[23] These and other guidelines limit both public and private data collection to the minimum necessary to accomplish a legitimate purpose.[24]

The United States Supreme Court is not in the habit of relying on international conventions to interpret constitutional provisions.[25] Nonetheless, one might hear echoes of these principles in Chief Justice John Roberts' approach to evaluating whether police need a warrant to search the cell phone contents of an arrestee in *Riley v. California*: "by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests."[26] Ira Rubenstein notes that Big Data "challenges international privacy laws in several ways: it casts doubt on the distinction between personal and non-personal data, clashes with data minimization, and undermines informed choice."[27] As the Supreme Court is beginning to recognize, Big Data challenges U.S. laws on privacy in the same ways.

Health information offers a paradigmatic candidate for exploring whether and when U.S. constitutional law should protect privacy. Information about a person's health can be viewed as intensely personal and private, access to which the person has a moral and perhaps legal right to control.[28] It can also be viewed as a valuable commodity that society needs in order to identify criminal suspects, investigate

---

23 *See* Robert Gellman, *Fair Information Practices: A Basic History* 3–8, 12–25 (Feb. 11, 2015), http://bobgellman.com/rg-docs/rg-FIPShistory.pdf.

24 *See* Maria Tzanou, *Data Protection as a Fundamental Right Next to Privacy? 'Reconstructing' a Not So New Right*, 3 INT'L DATA PRIVACY L. 88, 90 (2013) (distinguishing data protection and data privacy under the Lisbon Treaty); *International Principles on the Application of Human Rights to Communications Surveillance*, NECESSARY AND PROPORTIONATE (May 2014), https://en.necessaryandproportionate.org/text.

25 *See* James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1155–57, 1159–60 (2004) (explaining differences in EU and U.S. privacy law).

26 Riley v. California, 134 S. Ct. 2473, 2484 (2014) (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999)).

27 Ira S. Rubinstein, *Big Data: The End of Privacy or a New Beginning?*, 3 INT'L DATA PRIVACY L. 74, 74 (2013).

28 *See, e.g.*, EDWARD J. BLOUSTEIN, INDIVIDUAL AND GROUP PRIVACY 18 (1978); JUDITH WAGNER DECEW, IN PURSUIT OF PRIVACY: LAW, ETHICS, AND THE RISE OF TECHNOLOGY 1–2 (1997); JULIE C. INNESS, PRIVACY, INTIMACY, AND ISOLATION 3–4 (1992); Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 979 (1964); Joel Feinberg, *Autonomy, Sovereignty, and Privacy: Moral Ideas in the Constitution?*, 58 NOTRE DAME L. REV. 445, 454 (1983); Louis Henkin, *Privacy and Autonomy*, 74 COLUM. L. REV. 1410, 1423–24 (1974); James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 34, 54–5 (2003); Tzanou, *supra* note 24, at 92, 97; Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195–97 (1890).

epidemics, calculate budgets, monitor the quality of care, develop social policy, and conduct biomedical and behavioral research.[29] Conceptualizing the meaning of privacy of medical and health information is nearly as fraught as conceptualizing the meaning of privacy itself, and this article will not attempt to resolve an ultimate meaning.[30] Rather, the question explored here is whether the U.S. Constitution may impose any limits on state-compelled collection or use of identifiable personal health information for civil—non-law enforcement—purposes, and if so, when and why. Broad limits may impede important social advances. However, if health information is not protected at all, can there be protection for other types of information?[31]

When courts and scholars offer examples of matters that self-evidently deserve privacy protection, medical information is a prime example.[32] In the United States, however, information privacy in general and health information privacy in particular is subject to a fragmented collection of federal and state laws.[33] As Professor Nicolas P. Terry notes, discussions of health information privacy often

---

29 *See* Nicolas P. Terry, *Protecting Patient Privacy in the Age of Big Data*, 81 UMKC L. REV. 385, 392 (2012) (noting that health data is seen "as a major source of big data").

30 For a lucid summary and critique of general theories of privacy, see DANIEL J. SOLOVE, UNDERSTANDING PRIVACY (2008). Thoughtful scholarly treatments of theories of privacy include AMITAI ETZIONI, THE LIMITS OF PRIVACY (1999); ARTHUR R. MILLER, THE ASSAULT ON PRIVACY (1971); DAVID J. SEIPP, THE RIGHT TO PRIVACY IN AMERICAN HISTORY (1978); ALAN F. WESTIN, PRIVACY AND FREEDOM (1967); Charles Fried, *Privacy*, 77 YALE L.J. 475, 493 (1968); Richard A. Posner, *Privacy, Surveillance, and Law*, 75 U. CHI. L. REV. 245, 248 (2008); Robert C. Post, *Three Concepts of Privacy*, 89 GEO. L.J. 2087, 2087 (2001).

31 *See* MICHEL FOUCAULT, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON 195–217 (Alan Sheridan trans.) (1977) (arguing that governments sought to control people by placing under surveillance to encourage conformity with social norms); Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 17 (2008) ("The more power the state amasses, the more Americans need constitutional guarantees to keep governments honest and devoted to the public good.").

32 *See e.g.*, United States v. Westinghouse Elec. Corp., 638 F.2d 570, 577 (3d Cir. 1980) ("There can be no question that an employee's medical records, which may contain intimate facts of a personal nature, are well within the ambit of materials entitled to privacy protection."); SOLOVE, *supra* note 30, at 14 ("[I]f a conception of privacy were to omit things we commonly view as private—such as medical information, intimate marital secrets, and freedom from surveillance—theorists would likely reject the conception."); Terry, *supra* note 29, at 386 ("[H]ealth information technologies ('HIT') and patient privacy share a long history of bipartisan support."); *Electronic Health Data Exchanges: Patient and Consumer Principles for System Design*, MARKLE FOUNDATION (Oct. 11, 2005), http: / / www.markle.org/publications/878-electronic-health-data-exchanges-patient-and-consumer-principles-system-design (reporting wide support for patients to be able to refuse to share their health information). The Freedom of Information Act, 5 U.S.C. § 552(b)(6) (2012), specifically exempts medical files from disclosure.

33 *See* WENDY K. MARINER & GEORGE J. ANNAS, PUBLIC HEALTH LAW 398–401 (2014) (explaining various groundings for privacy rights); Ira S. Rubinstein et al., *Systematic Government Access to Personal Data: A Comparative Analysis*, 4 INT'L DATA PRIVACY L. 96, 96–97 (2014).

conflate privacy protection with preserving the confidentiality of information already obtained, with or without a person's permission.[34]

Calls for mandatory reporting of more health information, for example, typically contain the puzzling caveat that its collection and use should, of course, safeguard privacy.[35] There are, however, two separate issues here. The threshold question is whether identifiable data should be collected without consent in the first place. If not, its collection is an invasion of privacy.[36] The second is whether data that is properly obtained will be kept confidential—that is, not disclosed to others by the recipient. Discussions of mandatory reporting laws often proceed directly to the second question, skipping over the first.[37] Typically, the first question is waved away on the basis of a presumption that the state is free to compel reporting as long as it serves at least a legitimate state interest.[38] Thus, the concept of privacy is stripped of its normative force, leaving only procedural questions about whether and how to keep the reported information confidential—secure against further disclosure to unauthorized persons or the public at large.[39]

This focus on confidentiality or public disclosure also fails to ask a third or fourth question: whether the data should be used by the recipient for a different purpose than the one that justified its collection; or whether the recipient should be able to give the information

---

34 *See* Nicolas P. Terry, *What's Wrong with Health Privacy?*, 5 J. HEALTH & BIOMEDICAL L. 1, 5–8, 23–26 (2009).

35 Such comments are rarely accompanied by specific recommendations for privacy protection. *See, e.g.*, COMMITTEE ON THE RECOMMENDED SOCIAL AND BEHAVIORAL DOMAINS AND MEASURES FOR ELECTRONIC HEALTH RECORDS, CAPTURING SOCIAL AND BEHAVIORAL DOMAINS AND MEASURES IN ELECTRONIC HEALTH RECORDS: PHASE 2, at 13 (2014).

36 *See* RESTATEMENT (SECOND) OF TORTS §§ 652A-E (AM. LAW. INST. 1977); *see also id.* § 652A(2) ("The right of privacy is invaded by: (a) unreasonable intrusion upon the seclusion of another, as stated in § 652B; or (b) appropriation of the other's name or likeness, as stated in § 652C; or (c) unreasonable publicity given to the other's private life, as stated in § 652D; or (d) publicity that unreasonably places the other in a false light before the public, as stated in § 652E.").

37 *See, e.g.*, AMY L. FAIRCHILD ET AL., SEARCHING EYES: PRIVACY, THE STATE, AND DISEASE SURVEILLANCE IN AMERICA 1 (2007).

38 *See, e.g.*, Whalen v. Roe, 429 U.S. 589, 606 (1977) (Brennan, J., concurring). Some courts have used heightened scrutiny to require an important or even compelling state interest when the information at issue is especially sensitive, such as HIV infection or abortion. *See, e.g.*, Planned Parenthood of Cent. Mo. v. Danforth, 428 U.S. 52, 60–61 (1976); Sheets v. Salt Lake County, 45 F.3d 1383, 1388–89 (10th Cir. 1995); Walls v. City of Petersburg, 895 F.2d 188, 192 (4th Cir. 1990); Fraternal Order of Police v. City of Philadelphia, 812 F.2d 105, 110, 112–13 (3d Cir. 1987).

39 *See, e.g.*, The White House, Consumer Privacy Bill of Rights Act of 2015 [hereinafter Consumer Privacy Bill of Rights Act], www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf.

to third parties for new uses. Thus, there are at least four issues that deserve exploration: (1) the justification for the initial mandatory data collection; (2) security against further disclosure of the data (confidentiality); (3) permissible uses of the data collected; and (4) permissible disclosures of the data to third parties. The failure to distinguish these questions contributes to a lack of clarity surrounding what information warrants what, if any, kind of privacy protection.

This Article asks the first question: what kinds of information should government agencies be free to compel from third parties who hold an individual's personal health information? In other words, what counts as a justifiable intrusion on privacy? This is a question of constitutional power.

At first glance, the idea that mandatory reporting of health information might violate any constitutionally protected privacy interest or constitute an unreasonable search and seizure seems like an outdated notion. Judging from the volumes of articles on the topic, however, the question of the privacy of health-related information is not entirely settled. Yet the literature focuses on statutory and regulatory regimes, especially the HIPAA Privacy Rule.[40] The constitutional dimensions of health information privacy in the civil context have received little recent attention.[41]

---

40 Health Insurance Portability and Accountability Act ("HIPAA"): Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. § 164 (1996). *See also* Beverly Cohen, *Regulating Data Mining Post-*Sorrell*: Using HIPAA to Restrict Marketing Uses of Patients' Private Medical Information*, 47 WAKE FOREST L. REV. 1141, 1142 (2012); Frank Pasquale, *Grand Bargains for Big Data: The Emerging Law of Health Information*, 72 MD. L. REV. 682, 747–51 (2013); Frank Pasquale & Tara Adams Ragone, *Protecting Health Privacy in an Era of Big Data Processing and Cloud Computing*, 17 STAN. TECH. L. REV. 595, 597, 608 (2014); Mark A. Rothstein, *HIPAA Privacy Rule 2.0*, 41 J. L. MED. & ETHICS 525, 525 (2013); Lior Jacob Strahilevitz, *Toward a Positive Theory of Privacy Law*, 126 HARV. L. REV. 2010, 2021 (2013) (focusing on the positive law of privacy and empirical analyses of who wins and who loses). *But see* Mark A. Rothstein, *Constitutional Right to Informational Health Privacy in Critical Condition*, 39 J.L. MED. & ETHICS 280, 280–81 (2011) (describing due process challenges to demands for personal health information).

41 The focus of constitutional analysis has been NSA surveillance and law enforcement searches and seizures. *See generally* LORI ANDREWS, I KNOW WHO YOU ARE AND I SAW WHAT YOU DID: SOCIAL NETWORKS AND THE DEATH OF PRIVACY (2011); JAMES P. NEHF, OPEN BOOK: THE FAILED PROMISE OF INFORMATION PRIVACY IN AMERICA (2012); ROBERT O'HARROW, JR., NO PLACE TO HIDE (2005); FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION (2015); JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA (2000); CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT (2008); DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE (2004); DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY (2011).

Several indicators suggest that now is an opportune time to revisit the parameters of constitutional protection for health information. First, with a financial push from the federal government, health information is being digitized at an increasing rate, while private sector internet services allow individuals to upload and monitor their own health information via multiple devices.[42] All this feeds into Big Data, where predictive analytics can be used to identify higher quality, less costly health care and target individuals or groups for preventive or remedial interventions.[43]

Second, the excitement over Big Data's potential to improve our lives is tempered by concerns that information can be misused to the detriment of many people, especially the disadvantaged.[44] In this era, government agencies, including law enforcement and national security, can often obtain data collected by private entities.[45] Acknowledg-

---

42 The HITECH Act provides financial incentives for medical providers to adopt electronic medical records and permit data sharing. Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111–5, 123 Stat. 226, 226–27, 230 (codified as amended in scattered sections of 42 U.S.C.); *see also* THE OFFICE OF THE NATIONAL COORDINATOR FOR HEALTH INFORMATION TECHNOLOGY, REPORT TO CONGRESS ON HEALTH INFORMATION BLOCKING, at 4 (Apr. 2015), http:/ /www.healthit.gov/sites/default/files/reports/info_blocking_040915.pdf; *Health Datapalooza 2015 Continues to Focus on Access to Health Data*, HIMMS NEWS (June 5, 2015), http://www.himss.org/News/NewsDetail.aspx?ItemNumber=42579; Priyanka Dayal McCluskey, *Partners' $1.2b Patient Data System Seen as Key to Future*, THE BOSTON GLOBE (June 1, 2015), http://www.bostonglobe.com/business/2015/05/31/partners-launches-billion-electronic-health-records-system/oo4nJJW2rQyfWUWQlvydkK/story.html.

43 *See* Terry, *supra* note 29, at 723–24, 749–50; *see also* Stephen Blakely, *Measured Matters: The Use of "Big Data" in Employee Benefits*, NOTES, April 2015, at 11–12, 18 (describing analyses of employee health data by employers and health insurers); Girish Navani, *How Big Data is Driving the Consumerization of Health Care*, U.S. NEWS & WORLD REP. (Aug. 14, 2015), http://health.usnews.com/health-news/patient-advice/articles/2015/08/14/how-big-data-is-driving-the-consumerization-of-health-care (describing how wearable technology can be linked to medical records to improve patient care).

44 *See* JARON LANIER, WHO OWNS THE FUTURE? (2013) (describing the concentration of power among entities that control the collection and analysis of information); Frank Pasquale, *Resdescribing Health Privacy: The Importance of Information Policy*, 14 HOUS. J. HEALTH L. & POL'Y 95, 96–97 (2014) (describing potential discriminatory misuses of information). *See also* Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 12 (2008) (arguing that government is more likely to use surveillance to shape population behavior); Wendy K. Mariner, *The Affordable Care Act and Health Promotion: The Role of Insurance in Defining Responsibility for Health Risks and Costs*, 50 DUQ. L. REV. 271, 310–11 (2012) (describing the use of health information for wellness program rewards and penalties).

45 *See* Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309, 1320–21 (2012) ("The FBI and other law enforcement agencies will shift from being active producers of surveillance to passive consumers, essentially outsourcing all of their surveillance activities to private third parties, ones who are not only ungoverned by the state action requirements of the Fourth Amendment, but also who have honed the ability to convince private citizens to agree to be watched."); *see also* Balkin, *supra* note 44, at 7

ing such concerns, the Obama Administration proposed new statutory and regulatory measures to protect the privacy of data held by private data custodians, intensifying debate on the extent to which individuals should be able to control access to their personal information.[46] Moreover, members of Congress recently curbed the NSA's bulk data collection and other federal surveillance practices in order to limit privacy intrusions.[47] Most importantly, the Supreme Court's recent Fourth Amendment decisions suggest that a majority of Justices may be considering a more sophisticated approach to determining when government agencies can access digital data.

II. USES OF HEALTH INFORMATION

Health information is a valuable commodity. Properly collected and analyzed, it has the potential to provide insights into better quality, more efficient, and less costly health services.[48] It may also enable

("[T]he line between public and private modes of surveillance and security has blurred if not vanished. Public and private enterprises are thoroughly intertwined."); Amitai Etzioni, *The Privacy Merchants: What Is To Be Done?*, 14 U. PA. J. CONST. L. 929, 951 (2012) ("[O]ne must assume that what is private is also public in two senses of these words: that one's privacy (including sensitive matters) is rapidly corroded by the private sector and that whatever it learns is also available to the government."); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1095 (2002) ("[G]overnment is increasingly contracting with private sector entities to acquire databases of personal information.").

46 *See* Consumer Privacy Bill of Rights Act, *supra* note 39; *see also* President's Council of Advisors on Science and Technology, *Big Data and Privacy: A Technological Perspective* (May 2014), www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf; Federal Trade Commission, *Data Brokers: A Call for Transparency and Accountability* (May 2014), www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf; Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers (*March 2012), www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers; The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy (*Feb. 2012), www.whitehouse.gov/sites/default/files/privacy-final.pdf. The Centers for Medicare and Medicaid excised information concerning substance abuse from the claims records it opens to researchers. *See* Austin B. Frakt & Nicholas Bagley, *Protection or Harm? Suppressing Substance-Use Data*, 372 NEW ENG. J. MED. 1879, 1879 (2015) (arguing that researchers' lack of access to these files, representing about 4.5% of Medicare claims and 8% of Medicaid claims, will impede a wide range of research).

47 On June 2, 2015, Congress passed and the President signed the Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015, H.R. 2048, 114th Cong. § 201 (2015).

48 *See, e.g.*, Pasquale & Ragone, *supra* note 40, at 598; *see also* David W. Bates et al., *Big Data in Health Care: Using Analytics to Identify and Manage High-Risk and High-Cost Patients*, 33 HEALTH AFFAIRS 1123, 1123 (2014); Matthew Herland, Taghi M. Khoshgoftaar & Randall

individuals to access information about health concerns and the costs of care. Health informatics specialists suggest that achieving such goals is likely to entail integrating and analyzing data from different sources, such as medical records, gene banks, disease registries, public health databases, and social media to study both clinical and policy questions.[49] One might add to that list the data collected by commercial entities from individuals using wearable technologies like Fitbit to monitor distances walked, calories consumed, and the like.[50] The value of the results of such data mining and analysis, of course, depends importantly on the reliability and accuracy of the information contained in the source data sets.[51] However, the current state of technology is not immune from introducing new errors in the process of mining, integrating, and analyzing data.[52]

A. Clinical Medical Care, Payment for Services, and Health Care Operations

The original and still most common functions of electronic medical records ("EMR")—or electronic health records ("EHR"), the current, broader term—are (1) to make patient information available to clinicians and health care workers as needed to provide care to the patient,[53] and (2) to facilitate the submission and payment of provider claims for treatment services.[54] No one disputes the need for sharing identifiable patient information for these purposes, although there are some concerns that the shared information be limited to

---

Wald, *A Review of Data Mining Using Big Data in Health Informatics,* J. BIG DATA, June 2014, at 22; Sharona Hoffman & Andy Podgurski, *Improving Health Care Outcomes Through Personalized Comparisons of Treatment Effectiveness Based on Electronic Health Records*, 39 J.L. MED. & ETHICS 425, 425 (2011).

49 Hoffman & Podgurski, *supra* note 48, at 428; *see also* Nigam H. Shah& Jessica D. Tenenbaum, *The Coming Age of Data-Driven Medicine: Translational Bioinformatics' Next Frontier*, 19 J. AM. MED. INFORMATICS ASS'N e1, e3 (2012).

50 Angela Daley, *The Law and Ethics of 'Self-Quantified' Health Information: An Australian Perspective*, 5 INT'L DATA PRIVACY L. 144 (2015) (describing such devices and their uses).

51 *See* Sharona Hoffman, *Medical Big Data and Big Data Quality Problems*, 21 CONN. INS. L.J. 289, 290, 304 (2015); *see also* Simon I. Hay, Dylan B. George, Catherine L. Moyes & John S. Brownstein, *Big Data Opportunities for Global Infectious Disease Surveillance,* PLOS MED., Apr. 2013, at 2–3 (noting that data from social media can be unreliable or misleading).

52 Thomson Kuhn et al., *Clinical Documentation in the 21st Century: Executive Summary of a Policy Position Paper From the American College of Physicians*, 162 ANNALS INTERNAL MED. 301, 308 (2015). *See generally* K. Krasnow Waterman & Paula J. Bruening, *Big Data Analytics: Risks and Responsibilities*, 4 INT'L DATA PRIVACY L. 89, 89–90 (2014).

53 Kuhn et al., *supra* note 52, at 302, 310.

54 The "treatment" and "payment" uses are permitted without patient authorization under the HIPAA Privacy Rule as part of "treatment, payment or health care operations." 45 C.F.R. § 164.506 (2002).

only that necessary for the recipient to perform a specific function.[55] Most large hospital systems and large physician group practices have implemented EHRs, but adoption by smaller providers has been slow.[56] A lack of interoperability among EHR systems has hindered progress toward statewide, regional, and national networks.[57] Nonetheless, EHRs are expected to become the source of data for an increasing number of purposes as technology improves.[58]

Hospitals and other health care facilities, as well as physician practice groups, typically review EHR data to analyze the cost and quality of care they have provided to their patients. Such review can focus on a single patient—to identify an error in diagnosis, treatment or follow-up—or on a group of patients to determine whether a particular course of treatment has proved effective.[59] Where the analyses are designed to provide generalizable knowledge to improve patient care in general, rather than to inform the reviewers' own practices, they could be considered health services research that requires patient consent under state law.[60]

B. State Databases

States have developed several databases of identifiable health information for both clinical and research uses. The Federal Government encourages states to create Prescription Drug Monitoring Pro-

---

55 For a history and comparison of different versions of Fair Information Practices, see Gellman, *supra* note 23.

56 *See* Nicolas P. Terry & Leslie P. Francis, *Ensuring the Privacy and Confidentiality of Electronic Health Records*, 2007 U. ILL. L. REV. 681, 686 (2007).

57 *See id.* at 682.

58 *See* Caitlin M. Cusack et al., *The Future State of Clinical Data Capture and Documentation: A Report from AMIA's 2011 Policy Meeting*, 20 J. AM. MED. INFORMATICS ASS'N. 134 (2013). *But see* Jennifer Bresnick, *Health Information Exchange Data Scarce, Inaccurate, Incomplete*, HEALTH IT ANALYTICS (Feb. 17, 2015), http://healthitanalytics.com/news/health-information-exchange-data-scarce-inaccurate-incomplete ("Due to the perception of health information exchange as unpredictable, inaccurate, incomplete, and expensive, 70% of non-system hospitals and 91% of physician practices are not routinely communicating patient data to external organizations.").

59 Such reviews are encompassed under the "health care operations" uses permitted without patient authorization under the HIPAA Privacy Rule. 45 C.F.R. § 164.502(a), 45 C.F.R. § 164.506.

60 *But cf.* J. Cassel & A. Young, *Why We Should Not Seek Individual Informed Consent For Participation In Health Services Research*, 28 J. MED. ETHICS 313, 316 (2002) ("A right to individual informed consent, interpreted as an absolute requirement in all areas of research, militates against health care for disadvantaged minorities, since some groups will have the notional 'right' to health care but are not in a position to exert that right equally.").

grams ("PDMPs") in an effort to reduce prescription drug abuse.[61] Physicians can consult an electronic database of prescription drugs dispensed to individuals to determine whether a patient has a legitimate medical need for the drug. PDMPs, especially those that allow law enforcement or other government agencies access to the data, raise Fourth Amendment questions, discussed in Part V.

The need to control health care costs generated proposals for states to collect health insurance claims data, to analyze the cost of different types of health care services and items.[62] At least sixteen states have enacted legislation requiring health insurance companies to submit reports of their payments on behalf of enrollees to the state department of health or insurance or a special agency created to collect such reports in an All Payer Data Base ("APDB"), sometimes called an All Payer Claims Database ("APCD").[63]

More states are proposing or developing APDBs. Individuals whose data are reported are not asked for consent and may not even realize that their data is being sent to the state.[64] Most states outsource the operation of the APDB to an outside vendor.[65]

An additional stated goal of APDBs is to determine the quality of different approaches to care for medical conditions, but quality has been subordinated to cost concerns so far, perhaps because reliable measures of quality remain limited. To analyze quality, states may need to track the care provided on an individualized basis in order to

---

61 *See generally* Kristin M. Finklea et al., *Prescription Drug Monitoring Programs*, Congressional Research Service Report for Congress R42593 (Jan. 3, 2013).

62 *See* Jo Porter et al., *The Basics of All-Payer Claims Databases: A Primer for States*, STATE HEALTH AND VALUE STRATEGIES (Jan. 14, 2014), http://www.rwjf.org/en/research-publications/find-rwjf-research/2014/01/the-basics-of-all-payer-claims-databases—a-primer-for-states.html.

63 If truly all payers are included, then Medicare and Veterans Affairs health services, as well as other federal health benefit programs, need to agree to submit their claims for benefits. The Federal Government has been reasonably willing to participate, given its interest in finding ways to control health care costs. *See* MD. HEALTH CARE COMM'N & CTR. FOR ANALYSIS AND INFO. SERVS., *Draft Work Plan for Expanding the Content and Use of Maryland's Medical Care Data Base (MCDB) to Address New Information Needs*, at 2 (June 2013), http://mhcc.maryland.gov/mhcc/pages/apcd/apcd_mcdb/documents/MCDB_Draft_Workplan_20130601.pdf. (describing the history and operation of the Maryland Medical Care Data Base). Third party administrators ("TPAs") of self-funded employer-sponsored health plans governed by the Employee Retirement Income Security Act ("ERISA") present a different problem. *See* Gobeille v. Liberty Mut. Ins. Co., 136 S. Ct. 936 (2016) (finding that ERISA preempts Vermont state requirement that ERISA plans or their TPAs report claims).

64 Most health insurance policies include a standard provision that the policyholder agrees to allow the insurer to use and disclose the person's information for multiple purposes, with some explicitly including research. Sample policies are on file with author.

65 *See* Porter et al., *supra* note 62.

attribute outcomes to specific provider interventions. They may also wish to observe cost of care trends associated with particular patients or providers to impute rises or falls in cost (accounting for volume), with or without comparing the quality of the care provided. Both uses typically require tracking individual patients and which individual practitioners provided what type of care.

A major motivating idea behind APDBs is that states will be able to provide consumers with price information about particular health services, thereby enabling consumers to choose the most cost-effective health plans and providers. So far, however, the data has been used primarily for research, by the agencies and outside research organizations like universities and consulting firms, with limited information open to consumers.[66] There is considerable enthusiasm for APDBs among research organizations, which advocate making greater use of the data for multiple research purposes.[67] Proposals include linking the APDB to other databases, such as medical records, disease registries, vital statistics, and patient surveys.

There is no question that it would be useful to be able to identify what types of medical care work well and which do not—and at what price—both to improve patient care and to avoid wasting money. Doing so often requires following identifiable patients as they go from provider to provider. Indeed, supporters of APDBs advocate releasing identifiable data sets to providers and others for such purposes.

Databases invite data mining.[68] The appeal of analyzing information already collected is almost irresistible. If one searches hard enough, something will certainly be found. Thus, the mere existence of a database attracts new users and uses. Some of these uses may be

---

66 *See* D.J. Wilson, *New APCD Legislation Getting Broad Support*, STATE OF REFORM (Jan. 30, 2015), http://stateofreform.com/news/industry/healthcare-providers/2015/01/new-apcd-legislation-getting-broad-support/ ("One of the key talking points from supporters last year was that providing information options for consumers would help drive accountability and price reductions in the market. The new legislation makes the use of the data primarily for research purposes by academic institutions rather than for individuals in their health care decision making.").

67 *See, e.g.*, The Network for Excellence in Health Innovation ("NEHI"), *All Payer Claims Databases: Unlocking the Potential* (Dec. 2014), http://www.nehi.net/publications/62-all-payer-claims-databases-unlocking-the-potential/view ("Experts agreed that it was unlikely for APCDs to become the go-to resource for consumer price/cost transparency information."). NEHI's board of directors consists of executives of health insurance companies, academic medical centers, and commercial businesses.

68 *See generally* SIMSON GARFINKEL, DATABASE NATION: THE DEATH OF PRIVACY IN THE 21ST CENTURY (Deborah Russell ed., 1st ed. 2000); ROBERT O'HARROW, JR., NO PLACE TO HIDE (2005).

benign, but others may not be so benign.[69] New users develop a stake in the database. If any serious objection arises, these stakeholders often are too entrenched to support any limitation on data collection or uses.[70]

C. Public Health Surveillance

Much of the public, including privacy scholars and judges, probably are unfamiliar with modern public health surveillance programs, perhaps assuming that such programs are limited to serious epidemics of contagious disease, like Ebola or avian flu.[71] To be sure, all states have laws that require medical facilities, physicians, and laboratories to report diagnoses of contagious diseases that could pose a risk of infecting the public. The list of diseases and conditions that the Centers for Disease Prevention and Control recommend be reported has grown to sixty-nine, although not all states require all to be reported.[72] In the case of disease outbreaks, like the recent measles outbreaks, the reports help trace the cases to their source and health practitioners can intervene to stop the spread of disease.

Investigating outbreaks and epidemics, however, is a declining part of public health surveillance today.[73] Public health now focuses special attention on chronic diseases.[74] Many states require the reporting of individuals with non-infectious chronic diseases like asthma, multiple sclerosis, and lupus, in order to study whether they might be caused by environmental risks.[75] Most states also have regis-

---

69 *See, e.g.*, Aid for Women v. Foulston, 427 F. Supp. 2d 1093 (D. Kan. 2006) (rejecting state Attorney General's opinion that sexual abuse reporting statute required medical providers to report consensual sexual activity of minors to the state).

70 MARINER & ANNAS, *supra* note 33, at 432.

71 *See, e.g.*, Deven McGraw, Privacy Concerns Related to Inclusion of Social and Behavioral Determinants of Health in Electronic Medical Records, Appendix B, in IOM Report (summarizing HIPAA's public health exception without describing what counts as public health).

72 *See* Centers for Disease Prevention and Control ("CDC"), 2014 National Notifiable Infectious Diseases, http: / / wwwn.cdc.gov/NNDSS/script/ConditionList.aspx? Type=0&Yr= 2014. Recommendations are developed by the CDC and the Council of State and Territorial Epidemiologists, a professional membership association of state and local epidemiologists. The National Notifiable Disease Surveillance System at the CDC collects disease reports that are voluntarily submitted by the states. For a history of disease surveillance, see generally FAIRCHILD ET AL., *supra* note 37.

73 Wendy K. Mariner, *Mission Creep: Public Health Surveillance and Medical Privacy*, 87 B.U. L. REV. 347, 350 (2007).

74 World Health Organization, Preventing Chronic Diseases—A Vital Investment, at 2 (2005), http://www.who.int/chp/chronic_disease_report/contents/en/.

75 *See, e.g.*, CONN. GEN. STAT. § 10-206(f) (2014) (requiring schools to report the number of students with diagnosed Asthma cases, "(1) at the time of public school enrollment, (2)

tries that collect identifiable information about persons with various conditions, such as cancers, as well as immunization registries to identify children who have not received all the recommended vaccines.[76] All states require newborns to be screened for between six and thirty-one genetic and congenital conditions; two states allow parents to refuse the tests.[77] Most experts agree that screening is important for at least six of these conditions, including PKU and sickle cell, because some form of treatment is available to prevent or ameliorate the condition if begun in infancy.[78] The blood test samples and results for other conditions are retained for varying lengths of time in what amounts to a DNA bank and are used predominantly for research.[79] In 2014, however, federal legislation recognized that studies using newborn blood samples collected in newborn screening programs must comply with federal regulations governing research with human subjects, including obtaining consent for research uses.[80]

A more controversial example of chronic disease surveillance is New York City's Blood Sugar Registry. The City's Board of Health ordinance requires laboratories to report the results of every Hemoglobin A1c (blood sugar) test to the department of Health and Men-

---

in grade six or seven, and (3) in grade ten or eleven"); MD. CODE REGS. 11.17.03.02 (mandating licensees to report defined medical conditions including multiple sclerosis to the Motor Vehicle Administration). Other reporting statutes may be invoked for a limited time period and geographic area. *See* MASS. DEP'T OF PUB. HEALTH CTR. FOR ENVT'L EPIDEMIOLOGY PROGRAM, FINAL REPORT ON THE INCIDENCE AND PREVALENCE OF SYSTEMIC LUPUS ERYTHEMATOSUS ("SLE") IN BOSTON AND ENVIRONMENTAL FACTORS 3–8, (2007), http://www.mass.gov/eohhs/docs/dph/environmental/tracking/lupus-report-web.pdf (referring to data collected from in-patient and out-patient records from eleven major hospitals in the Metro-Boston catchment area that were obtained by requests pursuant statutory authority).

76 *See* National Program of Cancer Registries, 42 U.S.C. § 280e (2002) (authorizing the CDC to provide grants for creating cancer registries to states that have certain laws in place); IND. CODE § 16-38-2 (2004), https://iga.in.gov/legislative/laws/2014/ic/titles/016/ (establishing a cancer registry that is open for research purposes without consent unless the researcher seeks additional information in which case they must obtain the consent of the patient's attending physician and the written consent of the patient).

77 For specific screening requirements in each state, see About Newborn Screening/Conditions Screened by State, www.babysfirsttest.org/newborn-screening/states.

78 *See* STEFAN TIMMERMANS & MARA BUCHBINDER, SAVING BABIES: THE CONSEQUENCES OF NEWBORN GENETIC SCREENING (2013) (describing how newborn screening is done in practice); *see also* Leila Barraza & Lauren Burkhart, *The Expansion of Newborn Screening: Implications for Public Health and Policy*, 23 ANNALS HEALTH L. 42, 45–46 (2014).

79 *See* INSTITUTE OF MEDICINE, CHALLENGES AND OPPORTUNITIES IN USING RESIDUAL NEWBORN SCREENING SAMPLES FOR TRANSLATIONAL RESEARCH 51–54 (Steve Olson & Adam C. Berger, Rapporteurs 2010).

80 Newborn Screening Saves Lives Reauthorization Act of 2014, 42 U.S.C. § 300b-12 (amending 42 U.S.C. §§ 300b-1 et. seq.)

tal Hygiene by name without patient consent.[81] The department seeks the reports to identify individuals and ensure that they receive treatment for diabetes and behavioral education, although the individuals may already be under a physician's care, and the department cannot compel anyone to accept assistance.[82]

D. Research

The reader may have noticed a recurring theme in the above examples. A striking proportion of the uses of medical information collected is for research. Indeed, medical databases offer a cheaper alternative to conducting research studies with actual human beings.[83] That research ranges from biomedical and epidemiological studies by academic institutions to qualitative research on behavioral risks to health, such as tobacco and alcohol use, weight, substance abuse, and depression.[84] The data are also studied to develop government agency budgets, employment and other social policies, and whether to require more reporting.[85]

Many organizations encourage the collection and use of more health data electronically for multiple purposes, including research.[86] The Institute of Medicine recommended that research using health

---

81 New York City, N.Y., 24 Health Code §§ 13.03–04 (2006). For a description and critique of the Registry, see generally Wendy K. Mariner, *Medicine and Public Health: Crossing Legal Boundaries*, 10 J. HEALTH CARE L. & POL'Y 121 (2007).

82 Shadi Chamany et al., *Tracking Diabetes: New York City's A1C Registry*, 87(3) THE MILBANK QTRLY. 547, 559 (2009). Note that the registry does not track diabetes; it only requires reporting of blood sugar levels, one of several measures used to diagnose diabetes. Mariner, *supra* note 81, at 123.

83 Paul M. Schwartz, *Information Privacy in the Cloud*, 161 U. PA. L. REV. 1623, 1631–32 (2013).

84 *See generally* J.R. Lumpkin, *History and Significance of Information Systems and Public Health*, in PUBLIC HEALTH INFORMATICS AND INFORMATION SYSTEMS 16–38 (P.W. O'Carroll, W.A. Yasnoff, M.E. Ward, L.H. Ripp, & E.L. Martin, eds. 2003).

85 *See* Leslie P. Francis, *Patient Registries: Patient Consent When Patients Become Adults*, 7 ST. LOUIS U. J. HEALTH L. & POL'Y 389 (2014); A. Nosek et al., *Promoting an Open Research Culture*, 348 (6242) SCIENCE 1422 (2015) (advocating increased sharing of datasets for research).

86 *See, e.g.*, Committee on the Recommended Social and Behavioral Domains and Measures for Electronic Health Records, Institute of Medicine, *Capturing Social and Behavioral Domains and Measures in Electronic Health Records: Phase 2*, at 5 (2014); Kuhn, *supra* note 52, at 7 ("The laudable goal is to be able to extract data automatically from patient records, compile the data into reports, and export them with the click of a button. This process, if it worked well, would be far better than the current process of manual chart abstraction; additional data entry at the point of care; and dependency on claims data for measurement of quality, public health reporting, research, and regulatory compliance."); PriceWaterhouseCoopers, *Transforming Healthcare Through Secondary Use of Health Data* (2009), www.pwc.com/us/en/healthcare/publications/secondary-health.data.jhtml.

information should be permitted without the individual's consent.[87] That recommendation, criticized by some legal scholars, has not gained noticeable support outside the research community.[88] A recent report recommends that electronic health records include more information about a patient's social and behavioral issues to "enable more effective responses to the pressures [affecting health] when used by health systems, including public health officials, researchers, and providers treating individual patients."[89] Among the elements recommended to be noted in the medical record were stress, negative affect such as depression or anxiety, physical activity, alcohol use, exposure to partner violence, and socioeconomic characteristics, including neighborhood median household income.[90]

The commercial and research value of large databases of identifiable information can attract external threats to privacy. Health information appears to be surprisingly vulnerable to hacking, theft, and loss.[91] The Department of Health and Human Services posts reports of breaches of more than 500 medical records since 2009, required pursuant to the HITECH Act.[92] The site listed more than 1,000

87 BEYOND THE HIPAA PRIVACY RULE: ENHANCING PRIVACY, IMPROVING HEALTH THROUGH RESEARCH 42–43 (S.J. Nass, L.A. Levit & L.O. Gostin, eds. 2009) [hereinafter IOM RESEARCH] (arguing that research with identifiable health information should not require consent, in part because obtaining consent can be difficult and costly).

88 *See generally* Mark A. Rothstein, *Improve Privacy in Research by Eliminating Informed Consent? IOM Report Misses the Mark*, 37 J.L. MED. & ETHICS 507 (2009) (challenging the IOM recommendations on empirical and ethical grounds). For similar criticisms of proposals to use UK National Health Service data for research without patient consent, see generally Ian Brown, Lindsey Brown & Douwe Korff, *Using NHS Patient Data for Research Without Consent*, 2(2) LAW, INNOVATION & TECH. 219 (2011); Nikolaus Forgó, *My Health Data—Your Research: Some Preliminary Thoughts on Different Values in the General Data Protection Regulation*, 5 INT'L DATA PRIVACY L. 54 (2015).

89 NATIONAL ACADEMY OF SCIENCES, COMMITTEE ON THE RECOMMENDED SOCIAL AND BEHAVIORAL DOMAINS AND MEASURES FOR ELECTRONIC HEALTH RECORDS, INSTITUTE OF MEDICINE, CAPTURING SOCIAL AND BEHAVIORAL DOMAINS AND MEASURES IN ELECTRONIC HEALTH RECORDS: PHASE 2, at 3 (2014).

90 *Id.* at 8, Table S-1.

91 *See* PONEMON INSTITUTE, FOURTH ANNUAL BENCHMARK STUDY OF PATIENT PRIVACY & DATA SECURITY (Mar. 2014), www2.idexpertscorp.com/ponemon-report-on-patient-privacy-data-security-incidents/; Vincent Liu et al., *Data Breaches of Protected Health Information in the United States* (Research Letter), 313 J. OF THE AM. MED. ASS'N 1471 (2015); *see also* Dep't of Health and Human Services, Office of Civil Rights, *Improper Disclosure of Research Participants' Protected Health Information Results in $3.9 Million HIPAA Settlement* (Mar. 17, 2016), http://www.hhs.gov/about/news/2016/03/17/improper-disclosure-research-participants-protected-health-information-results-in-hipaa-settlement.html#.

92 Health Information Technology for Economic and Clinical Health Act, 42 U.S.C. §§ 201 *et seq.*, Pub. L. 111-5, 123 Stat. 226.

breach reports as of February 2015.[93] Each report covers a breach of hundreds, thousands and sometimes millions of records.[94]

This overview should demonstrate how the uses of health information—current as well as prospective—are expanding with the growth in technology, exacerbating tensions between privacy and Big Data. Statutory and common law protections for patient information remain patchy.[95] While privacy advocates seek greater privacy protection, powerful public and private institutions encourage legislation to expand their access to health information. Hence, the time is ripe to reconsider whether there are any constitutional limits to government collection and use of health information.

III. THE FOURTH AMENDMENT AND THE THIRD-PARTY DOCTRINE

We might begin with the presumption that the Fourth Amendment[96] does not apply when government compels an entity to produce another person's health information. In other words, such a search is an exception to the Fourth Amendment. Two lines of cases

---

93 *Breaches Affecting 500 or More Individuals*, U.S. DEP'T OF HEALTH AND HUMAN SERVICES OFFICE FOR CIVIL RIGHTS, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Nov. 11, 2015).

94 For example, hackers broke into the electronic database of information about Anthem Inc. (formerly Wellpoint) health insurance enrollees. Anthem's stored database, which contained eighty million unencrypted Social Security numbers of enrollees, was not encrypted, reportedly because encryption would make it harder to share enrollee information with health providers and state agencies. Danny Yadron & Melinda Beck, *Health Insurer Anthem Didn't Encrypt Data in Theft*, WALL ST. J. BLOG (Feb. 5, 2015, 7:26 PM), http://www.wsj.com/articles/investigators-eye-china-in-anthem-hack-1423167560. Hospitals and insurers use random passwords and other mechanisms to enable authorized access to patient records in their own internal central database; but the databases themselves, where records are stored electronically, may or may not be encrypted or otherwise unusable to hackers. Anthem, undoubtedly like some other companies, may have decided that information security was not worth the cost. *Id.* Whatever the reason, some companies may find sharing the information more important than safeguarding patient privacy.

95 Latanya Sweeney analogized legal protections for privacy in general to placing a few cloth patches randomly on the body instead of dressing it in a whole suit of clothes. Latanya Sweeney, Presentation, University of Pennsylvania Journal of Constitutional Law Symposium, "What Privacy? Exploring a Constitutional Right to Information Privacy," cosponsored by the American Bar Association Section of Individual Rights & Responsibilities, Jan. 23, 2015.

96 The Fourth Amendment states that

> [t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST., amend. IV.

support this presumption. First, the third-party doctrine has effectively excised information obtained from third parties from Fourth Amendment protection.[97] The third-party doctrine presumes that information held by third parties, like hospitals and health insurers, no longer qualifies as the person's "papers or effects" protected by the Fourth Amendment.[98] Second, the special needs doctrine has created another exception, which has expanded to permit government invasions of privacy for increasingly questionable reasons.[99] Thus, it is not surprising that most observers would assume that the Fourth Amendment does not protect health information to any cognizable degree.[100]

However, neither line of cases squarely addresses the question whether government can compel the production of personally identifiable health information for civil purposes.[101] The third-party doctrine developed in the context of criminal procedure—investigations and prosecutions—which is the subject of most Fourth Amendment scholarship.[102] Recent special needs cases have considered

97 *See* Smith v. Maryland, 442 U.S. 735, 741 (1979); United States v. Miller, 425 U.S. 435, 440 (1976).

98 *See* State v. Davis, 12 A.3d 1271, 1273 (N.H. 2010) (finding no reasonable expectation of privacy in medical test results provided to law enforcement); People v. Perlos, 462 N.W.2d 310, 321 (Mich. 1990) (relying on *United States v. Miller* to find that patients had no possession, or ownership, or reasonable expectation of privacy in blood test results for alcohol levels that hospital turned to police in automobile accident investigation). This presumption is subject to a growing number of critiques. *See* United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (noting that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties"); Jace C. Gatewood, *It's Raining* Katz *and* Jones*: The Implications of* United States v. Jones*—A Case of Sound and Fury*, 33 PACE L. REV. 683, 684–85 (2013); *see generally* Stephen E. Henderson, *The Timely Demise of the Fourth Amendment Third Party Doctrine*, 96 IOWA L. REV. BULL. 39 (2011).

99 *See infra* Part V; *see generally* Bd. of Educ. of Indep. Sch. Dist. v. Earls, 536 U.S. 822 (2002).

100 *See, e.g.*, Hoffman & Podgurski, *supra* note 1, at 111 ("The Supreme Court has not found that patients have either a property right or a privacy right associated with their medical records."); Neil M. Richards, *Why Data Privacy Law Is (Mostly) Constitutional*, 56 WM. & MARY L. REV. 1501, 1505 (2015); Marc A. Rodwin, *Patient Data: Property, Privacy & the Public Interest*, 36 AM J. L. & MED. 586, 588 (2010); Edward P. Richards, *Collaboration Between Public Health and Law Enforcement: The Constitutional Challenge*, 8 EMERGING INFECTIOUS DISEASES 1157, 1157 (Oct. 2002), http:/ /www.cdc.gov/ncidod/EID/vol8no10/02-0465.htm ("[U]nder the police power, public health officials . . . may search and seize without probable-cause warrants.").

101 Fourth Amendment challenges to government access to health information are rare. *But see* United States v. Warshak, 631 F.3d 266, 274 (6th Cir. 2010); Doe v. Broderick, 225 F.3d 440, 443 (4th Cir. 2000); State v. Skinner, 10 So.3d 1212, 1213 (La. 2009); New York City Health & Hospital Corp. v. Morgenthau (In re Grand Jury Investigation), 779 N.E.2d 173, 174 (N.Y. 2002); People v. Perlos, 436 N.W.2d 310, 311 (Mich. 1990).

102 The literature on this topic is vast. *See generally* WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT (5th ed. 2014); SLOBOGIN, *supra* note 41; Susan

suspicionless searches for civil purposes, but such searches were bodily invasions—testing for unlawful drug use—not searches for data.[103] Thus, it is worth reviewing the scope and limits of these doctrines to see whether or how they might apply to laws mandating the reporting of health information and whether there is room for any Fourth Amendment protection.

As a preliminary matter, it should be noted that the Fourth Amendment makes no textual distinction between civil and criminal searches.[104] As Justice Byron White wrote in *Camara v. Municipal Court*, "It is surely anomalous to say the individual and his private property are fully protected by the Fourth Amendment only when the individual is suspected of criminal behavior."[105] The U.S. Supreme Court has certainly applied the Fourth Amendment in the civil context.[106] Thus, it cannot be assumed that the Fourth Amendment offers no protection to personal health information *solely* because the information is sought for purposes other than law enforcement.

Furthermore, demanding information directly from an individual certainly qualifies as a search of the person or his papers or effects.[107] A compulsory reporting law would constitute a search or a seizure under the Fourth Amendment if the requirement were directed at

---

Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3 (2007); Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us, Too*, 34 PEPP. L. REV. 975 (2007); Lucas Issacharoff & Kyle Wirshba, *Restoring Reason to the Third Party Doctrine*, 100 MINN. L. REV. 987 (2016); Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009); Matthew D. Lawless, *The Third Party Doctrine Redux: Internet Search Records and the Case for a "Crazy Quilt" of Fourth Amendment Protection*, 11 UCLA J. L. & TECH. 1 (2007); Solove, *supra* note 45.

103 *But see* Ferguson v. City of Charleston, 532 U.S. 67, 69 (2001). *See also infra* Part V.

104 Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 758 (1994) ("[T]he Fourth Amendment applies equally to civil and criminal law enforcement."); Delaney, *supra* note 9, at 11 ("[The] Fourth Amendment . . . unquestionably regulates all elements of federal and state government.").

105 Camara v. Municipal Court of S.F., 387 U.S. 523, 530 (1967).

106 *See, e.g.*, Soldal v. Cook Cnty., 506 U.S. 56, 60, 67 (1992) (confirming that the Fourth Amendment applies in the civil context and finding that police seizure of tenants' trailer at landlord's request prior to eviction hearing constitutes a seizure subject to Fourth Amendment); New Jersey v. T.L.O., 469 U.S. 325, 335 (1985) ("[T]his Court has never limited the Amendment's prohibition on unreasonable searches and seizures to operations conducted by the police."); Marshall v. Barlow's Inc., 436 U.S. 307, 321–24 (1978) (holding that the Fourth Amendment applies to administrative inspections of private commercial property); Warden v. Hayden, 387 U.S. 294, 301–02 (1967) (noting that the Fourth Amendment applies to searches and seizures regardless of how the matter taken is used).

107 *See* Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 506 (2007).

the person whose information is demanded.[108] Of course, health information is typically (although not always) held by a third party, such as a medical provider, a laboratory, an insurer, or (these days) an Internet server.[109]

Two questions arise here. The first is whether the location of the information makes a difference. The third-party doctrine says that it does, but criticism of that conclusion is mounting.[110] The second and perhaps more important question is whether the person has a reasonable expectation of privacy in personal information held by a third party. Each of these questions is discussed below.

A. The Third-Party Doctrine and Continuous Reporting

For decades, the third-party doctrine has operated to close the courts to claims that information provided to government by a third party violates the Fourth Amendment—primarily in the criminal context.[111] The doctrine's origins are attributed to *United States v. Miller*, in which federal Alcohol, Tobacco, and Firearms ("ATF") agents issued a subpoena *duces tecum* to a bank to obtain Miller's bank records, and the bank turned over the records.[112] The ATF was conducting a criminal investigation into suspected tax fraud by Miller, who allegedly owned an unregistered still and failed to pay whiskey taxes. The

---

108 *Hayden*, 387 U.S. at 301–02 (stating that Fourth Amendment applies to searches and seizures regardless of how the matter taken is used). Whether such a search would be reasonable without consent, a warrant, or a court order is a separate issue.

109 *See generally* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531 (2005) (discussing whether electronic searches of computer data should be deemed searches or seizures); *see also* United States v. Jacobsen, 466 U.S. 109, 113 (1984) ("A 'search' occurs when an expectation of privacy that society is prepared to consider reasonable is infringed. A 'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property."). Many people are keeping their own personal health records separately, such that health care providers are no longer the sole record keepers of health data. *See* ERIC TOPOL, THE PATIENT WILL SEE YOU NOW (2015) (arguing, optimistically, that a new era of mobile devices should enable individuals to perform their own diagnostic tests). Some health records compiled by individuals for themselves, however, may be stored in the cloud in a personal account or through a commercial provider of health monitoring services—who might or might not also be considered third parties—and an individual might have several such electronic storage sites. *See* Nicolas P. Terry, *Personal Health Records: Directing More Costs and Risks to Consumers?*, 1 DREXEL L. REV. 216 (2009) (comparing electronic health eecords to personal health records).

110 *See generally* SLOBOGIN, *supra* note 41; Freiwald, *supra* note 102; Henderson, *supra* note 98; Lawless, *supra* note 102.

111 *See, e.g.*, Smith v. Maryland, 442 U.S. 735 (1979).

112 United States v. Miller, 425 U.S. 435, 437–38 (1976).

Supreme Court found that the Fourth Amendment did not protect bank records from disclosure pursuant to a grand jury subpoena:

> This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[113]

In *Miller*, the Court concluded that there was no reasonable expectation of privacy in checks, which were "not confidential communications but negotiable instruments to be used in commercial transactions."[114]

Since *Miller*, it has been generally presumed that a person who voluntarily discloses information to a third party, like a bank or an internet service provider, knowing that the third party would use that information in its regular business, abandons his or her expectation of privacy in that information and thus, any Fourth Amendment protection against government access to the information.

Smith v. Maryland strengthened that assumption when it upheld the installation of a pen register at a telephone company's central office to monitor the telephone numbers dialed by a man suspected of making threatening and obscene calls to a robbery victim.[115] The telephone company acted on a request by police, who had no warrant or court order.[116] This warrantless search provided the evidence for a warrant to search Smith's home, where more evidence led to Smith's arrest and conviction for the robbery.[117]

The Supreme Court gave several reasons for finding that the Fourth Amendment posed no bar to the telephone company's compliance with the police request. First, the Court distinguished the pen register from the listening device attached to a public phone booth, which was at issue in *Katz*,[118] on the ground that the pen register recorded only numbers dialed and not any communication, spoken words, or content.[119] Second, it doubted whether "people in

---

113 *Id.* at 443.

114 *Id.* at 442.

115 *Smith*, 442 U.S. at 737.

116 *Id.*

117 *Id.*

118 Katz v. United States, 389 U.S. 347 (1967); *see also* Mancusi v. DeForte, 392 U.S. 364, 368 (1968) (adopting Justice John M. Harlan's concept of reasonable expectation of privacy from his concurrence in *Katz*, 389 U.S. at 361 (Harlan, J., concurring)).

119 *Smith*, 442 U.S. at 741 ("Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers." (quoting United States v. N.Y. Tel. Co., 434 U.S. 159, 167 (1977))).

general entertain any actual expectation of privacy in the numbers they dial."[120] Third, it noted that telephone companies routinely used pen registers for billing and other regular business purposes.[121] Finally, the Court concluded that it "consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[122]

Miller and *Smith* suggest that a patient who voluntarily gives personal information to a health care provider has no Fourth Amendment claim against any action by government to obtain that information from the provider. After all, the patient has voluntarily provided the information, and the provider is using it in the course of business—treating the patient and billing for treatment.

A closer look at the third-party doctrine line of cases, however, reveals that they rely on facts that differ from mandatory reporting laws in several important respects. First, the third-party doctrine developed in cases involving targeted criminal investigations; that is, law enforcement sought to obtain information about a person suspected of a criminal offense[123] or to identify the perpetrator of a crime.[124] In contrast, government agencies, such as health departments, seek mandatory reporting laws to collect health information for civil purposes.[125] Civil reporting laws require information about a population, none of whose members are suspected of any criminal offense. Second, the criminal cases involved one-off investigations, whereas reporting laws authorize data collection on an on-going basis.

Third, most third-party doctrine cases concerned information provided more or less voluntarily by the third party to law enforcement.[126] In contrast, mandatory reporting laws directly compel the

120 *Id.* at 742.

121 *Id.*

122 *Id.* at 743–44 (citing United States v. Miller, 425 U.S. 435, 442–44 (1976); Couch v. United States, 409 U.S. 322, 335–36 (1973); United States v. White, 401 U.S. 745, 752 (1971); Hoffa v. United States, 385 U.S. 293, 302 (1966); Lopez v. United States, 373 U.S. 427 (1963)).

123 *White*, 401 U.S. at 746–47 (false friends); *Hoffa*, 385 U.S. at 297–300 (same).

124 *Smith*, 442 U.S. at 737–38.

125 *See supra* Part II. Some civil purposes would justify mandatory reporting, just as people may have no reasonable expectation of privacy in some of their information; these issues are taken up in Part VII.

126 To be sure, entities providing information in response to a subpoena, as in *Miller*, might not feel that production is truly voluntary, even if they are able to contest the subpoena. And federal law required the bank in *Miller* to maintain the records in the first place, further diluting the meaning of "voluntary" in that case.

third party to turn data over to government.[127] Thus, mandatory reporting laws can be seen as government-compelled, continuous, suspicionless searches of an entire population's data, which *Miller* and its progeny never considered.[128] This looks like a contemporary analogy to the general warrant that the Founders crafted the Fourth Amendment to prevent, with the search conducted digitally rather than physically in the home.[129]

The NSA's bulk collection of data offers a contemporary analogy in the criminal context. The NSA relied on *Smith* to support the constitutionality of its program, but the legality, as well as the wisdom, of that program remains highly controversial.[130] If *Smith* is ultimately determined to not to justify bulk data collection for purposes of investigating terrorism, the third-party doctrine may prove to be fragile support for bulk data collection for civil purposes, too.[131]

There is a striking similarity between civil surveillance programs and the NSA's bulk collection program. Both § 215 of the Patriot Act and most mandatory reporting laws require the ongoing suspicionless collection of data for future data mining.[132] Yet one federal circuit court of appeals found the NSA's program was not authorized by the

---

127 *See* Lebron v. Sec'y of Fla. Dep't of Children and Families, 772 F.3d 1352, 1376 (11th Cir. 2014).

128 *Miller*, 425 U.S. at 444–45 n.6 ("There was no blanket reporting requirement of the sort we addressed in *Buckley v. Valeo*, 424 U.S. 1, 60–84 (1976). . . . We are not confronted with a situation in which the Government, through 'unreviewed executive discretion,' has made a wide-ranging inquiry that unnecessarily '[touch]es upon intimate areas of an individual's personal affairs.' *California Bankers Assn. v. Shultz*, 416 U.S. 21, 78–79 (Powell, J., concurring). Here the Government has exercised its powers through narrowly directed subpoenas *duces tecum* subject to the legal restraints attendant to such process." (alteration in original)).

129 *See* TECH. & PRIVACY ADVISORY COMM., U.S. DEP'T OF DEF., SAFEGUARDING PRIVACY IN THE FIGHT AGAINST TERRORISM 49 (2004), www.cdt.org/security/usapatriot/20040300tapac.pdf ("If conducted without an adequate predicate, [data mining] has the potential to be a twenty-first century equivalent of general searches, which the authors of the Bill of Rights were so concerned to protect against."); *see also* Andresen v. Maryland, 427 U.S. 463, 480 (1976) (noting that the Fourth Amendment prohibits general warrants, whereby government conducts "a general, exploratory rummaging in a person's belongings").

130 *See* ACLU v. Clapper, 785 F.3d 787, 826 (2d Cir. 2015) (finding § 215 of the Patriot Act does not authorize the bulk metadata collection program); Klayman v. Obama, 957 F. Supp. 2d 1, 42 (D.D.C. 2013) (finding that § 215 probably violates the Fourth Amendment).

131 *See* Rehberg v. Paulk, 611 F.3d 828, 847 (11th Cir. 2010) (noting "whether the analytical framework, much less the rationale" of *Smith* applies to modern technologies "is questionable and far from clearly established").

132 *See Clapper*, 785 F.3d at 795–97 (noting also the requirement that the data be kept confidential within the agency and not released except in accordance with strict policies).

Act.[133] Of particular interest is that court's discussion of what is "relevant" to an investigation.[134] The court concluded that the word "relevant" in § 215 referred only to a particular investigation, not to the ongoing collection of all metadata just in case it might prove useful in the future.[135] It found that "such an expansive concept of 'relevance' is unprecedented and unwarranted."[136]

Mandatory health data reporting laws are based on a similarly expansive concept of relevance. Substitute "medical research" for "criminal investigation," and the court's explanation could describe many health surveillance programs. For example, newborn screening databases are used primarily for research, and APDBs are used to analyze whether various approaches to health care are cost-effective. In some states, law enforcement can access PDMPs to obtain data about possible illegal drug users or prescribers.[137] Ironically, the NSA collects less specific information about individuals than do health surveillance programs. The NSA collected metadata—only telephone numbers and email addresses—not the content of calls or emails.[138] Surveillance programs collect names, addresses, test results, and a host of other details.[139]

Might *ACLU v. Clapper* suggest that civil surveillance programs are at risk? The relevance of the concept of "relevance" in civil surveillance programs lies in the justification for the initial data collection (question one above). Data are sought for a reason. Usually data are said to be "needed" for a particular purpose, such as investigating the source of an outbreak.[140] For databases like PDMPs and ACDBs, how-

---

133 *Id.* at 792.

134 Under the Patriot Act, the government may apply for an order requiring the production of any "tangible things" if it has reasonable grounds to believe that such things "are relevant to an authorized investigation," 50 U.S.C. § 1861(b)(2)(A), "to protect against international terrorism or clandestine intelligence activities," *id.* § 1861(a)(1). The scope of the application is the same as that of a subpoena *duces tecum* issued by a court for a grand jury investigation. *Id.* § 1861(c)(2)(D).

135 *Clapper*, 785 F.3d at 815 (finding that the text of § 215 did not permit sweeping up "a vast trove of records of metadata concerning the financial transactions or telephone calls of ordinary Americans to be held in reserve in a data bank, to be searched if and when at some hypothetical future time the records might become relevant to a criminal investigation").

136 *Id.* at 812.

137 Finklea et al., *supra* note 61, at 3.

138 *Clapper*, 785 F.3d at 793. The court also noted that even metadata could permit inferences about content in some instances. *Id.* at 794 & n.1 (citing Yves-Alexandre de Montjoye et al., *Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata*, 347 SCIENCE 536, 536 (2015)).

139 MARINER & ANNAS, *supra* note 33, at 456–57, 460, 544.

140 *Id.* at 459.

ever, the stated need is similar to the NSA's claims of relevance to an investigation. Of course, the NSA was looking for terrorists, not epidemics or data for medical research. Could this mean that ongoing data collection for criminal purposes violates a reasonable expectation of privacy, while doing the same for civil purposes does not?

A final difference between the third-party doctrine line of cases and mandatory health reporting laws lies in attitudes towards the information at issue. The third-party doctrine cases conclude that the person whose information is held by a third party has either voluntarily abandoned all control over the information or no longer has any legitimate property interest or reasonable expectation of privacy in the information.[141] Neither of these presumptions completely squares with public attitudes about health information.[142] As to the expectation of privacy, most patients expect that physicians, hospitals and insurers will not disclose identifiable data to the government unless the government has an independently justifiable basis for requiring the disclosure—beyond the mere fact that it exists in a medical record held by a third party.[143] State and federal laws protecting the confidentiality of medical records, from the common law duty of confidentiality[144] to the HIPAA Privacy and Security Rule,[145] support protecting

141 Smith v. Maryland, 442 U.S. 735, 73–74 (1979); United States v. Miller, 425 U.S. 435, 442 (1976); United States v. White, 401 U.S. 745, 749 (1971); Hoffa v. United States, 385 U.S. 293, 302 (1966).

142 *See* MARY MADDEN, PEW RESEARCH CTR. PUBLIC PERCEPTIONS OF PRIVACY AND SECURITY IN THE POST-SNOWDEN ERA, at 32 (2014), http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/ (reporting a 2014 survey's findings that, after social security numbers (90% very sensitive), respondents reported that their health status and medication information is very sensitive (55%) or somewhat sensitive (26%); phone conversations were similar (54% very sensitive; 27% somewhat sensitive), as well as email messages (52% very sensitive; 25% somewhat sensitive)); *see also* David Alan Sklansky, *Too Much Information: How Not to Think About Privacy and the Fourth Amendment*, 102 CAL. L. REV. 1069, 1110 (2014) (arguing that the Supreme Court is "wrong to declare that an individual can have no 'legitimate expectation of privacy' in anything shared voluntarily with someone else," in part because individuals have different privacy expectations and needs from different entities).

143 *See, e.g.*, Whalen v. Roe, 429 U.S. 589, 599 (1977) (recognizing "the individual interest in avoiding disclosure of personal matters"); Tucson Woman's Clinic v. Eden, 371 F.3d 1173, 1179, 1192 (9th Cir. 2004) (finding that laws authorizing health department access to abortion clinic patient records constitute unreasonable searches, because patients and physicians have a heightened expectation of privacy in medical information; and that abortion clinics were not a regulated industry subject to administrative search standards); State v. Skinner, 10 So.3d 1212, 1218 (La. 2009) (noting that "the right to privacy in one's medical and prescription records is an expectation of privacy that society is prepared to recognize as reasonable" under the Fourth Amendment).

144 *See e.g.*, Fort Wayne Women's Health v. Bd. of Commissioners, Allen Cnty., Indiana, 735 F. Supp. 2d 1045, 1057 (N.D. Ind. 2010) ("Medical patients have an actual expectation of privacy in their medical records and society sees this expectation as reasonable."); Alberts

health information from unauthorized disclosure. Such laws reflect societal acceptance that the expectation of privacy is objectively reasonable.

As to voluntarily abandoning control over one's information, numerous scholars observe that almost all activities of daily life require people to trust their identifiable information with third parties, such as banks, cable service providers, and retailers.[146] The overwhelming majority of Americans seek health care every year.[147] Individuals have no choice but to allow their health care providers and insurers to hold identifiable information about them—increasingly in digital format.

Two of the four dissenting Justices in *Smith* unsuccessfully pressed a related argument in 1979. Justice Thurgood Marshall, joined by Justice William J. Brennan, rejected the *Smith* majority's reasoning that people who give information to third parties "assume the risk" that their information will be conveyed to government.[148] Assump-

---

v. Devine, 479 N.E.2d 113, 118 (Mass. 1985) ("We continue to recognize a patient's valid interest in preserving the confidentiality of medical facts communicated to a physician or discovered by the physician through examination."); Bd. of Med. Quality Assurance v. Gherardini, 93 Cal. App. 3d 669, 679 (Cal. Ct. App. 1979) ("The state of a person's gastrointestinal tract is as much entitled to privacy from unauthorized public or bureaucratic snooping as is that person's bank account, the contents of his library or his membership in the NAACP."); *see also* Doe v. Broderick, 225 F.3d 440, 450 (4th Cir. 2000) (requiring a warrant to access medical/prescription records); United States v. Westinghouse Elec. Corp., 638 F.2d 570, 577 (3d Cir. 1980) ("There can be no question that an employee's medical records, which may contain intimate facts of a personal nature, are well within the ambit of materials entitled to privacy protection."); John B. v. Superior Court, 137 P.3d 153, 166–67 (Cal. 2006) (the right to privacy extends to medical records).

145 45 C.F.R. § 160.202(1)(4); 45 C.F.R. § 164.105(a)(2)(ii)(A); *see also* In the Matter of Miguel M., 950 N.E.2d 107 (N.Y. 2011) (rejecting argument that the HIPAA Privacy Rule permitted government to obtain medical records without a court order); Nw. Mem'l Hosp. v. Ashcroft, 362 F.3d 923, 924, 928–29 (7th Cir. 2004) (quashing a government subpoena for abortion records and noting that compliance would be "an invasion of privacy"). Other federal laws can affect health records. *See, e.g.*, Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-233; 42 U.S.C. § 290dd-2(a); *see also* Sam Kamin, *The Private is Public: The Relevance of Private Actors in Defining the Fourth Amendment*, 46 B.C. L. REV. 83, 85 (2004) (arguing that conceptions of privacy in the private sector should influence expectations of privacy under the Fourth Amendment).

146 *See* PASQUALE, *supra* note 41, at 4–5; David Cole, *Preserving Privacy in a Digital Age: Lessons of Comparative Constitutionalism*, *in* SURVEILLANCE, COUNTER-TERRORISM AND COMPARATIVE CONSTITUTIONALISM (Fergal Davis et al., eds., 2013); Stephen E. Henderson, *After* United States v. Jones*, After the Fourth Amendment Third Party Doctrine*, 14 N.C. J. L. & TECH. 431, 435 (2013) ("We now live in a world of ubiquitous third party information.").

147 John R. Pleis et al., Nat'l Ctr. for Health Statistics, *Summary Health Statistics for U.S. Adults: National Health Interview Survey, 2009*, *in*, 10 VITAL & HEALTH STAT. 1, 124 (2010), http://www.cdc.gov/nchs/data/series/sr_10/sr10_249.pdf.

148 Smith v. Maryland, 442 U.S. 735, 752 (1979) (Marshall, J. dissenting).

tion of risk, he argued, implies "some notion of choice,"[149] which does not exist where a person has "no realistic alternative" to using a "personal or professional necessity" like a telephone.[150] Instead, he continued, the question is not what risks a person should be presumed to accept, but "the risks he should be forced to assume in a free and open society."[151]

These features of mandatory reporting laws—ongoing population-wide, suspicionless searches for civil uses and today's practical necessity of giving health information to third parties—contrast significantly with the assumptions underlying the third-party doctrine. The distinctions suggest that there may be room for Fourth Amendment protection of identifiable health data held by health, insurance or internet service providers—at least in some circumstances.[152] To explore the feasibility of such protection, it may help to know which elements of the third-party doctrine are essential to its retention. If those elements are no longer plausible, then the doctrine need not apply in all circumstances.

B. Third-Party Doctrine Rationales

The Supreme Court has offered various, but not always consistent, reasons for applying the third-party doctrine.[153] One is that a person has voluntarily abandoned his information to the third party. This equates telling one's physician about physical or mental symptoms with leaving the trash out for pickup.[154] It strains credulity to think that a person who confides in her physician believes she is throwing out her personal information for anyone to see.

Another way of viewing the concept of abandonment of one's information is to posit that a person who tells another person something necessarily (and thus voluntarily) consents to the further distri-

149 *Id.* at 749.

150 *Id.* at 750. Echoes of Justice Marshall's arguments may be found in *Riley v. California*, 134 S. Ct. 2473 (2014) and *United States v. Jones*, 132 S. Ct. 945 (2012). *See infra* text accompanying notes 162–69.

151 *Smith*, 442 U.S. at 750 (Marshall, J., dissenting).

152 For arguments that the third-party doctrine should be modified or abandoned in the criminal context, see LAFAVE, *supra* note 102, § 2.7 (criticizing *Miller*); *see also* Freiwald, *supra* note 102; Henderson, *supra* note 98; Lawless, *supra* note 102. For arguments favoring retaining the doctrine, see generally Kerr, *supra* note 102.

153 *See* Kerr, *supra* note 107, at 506 (arguing that the Court actually uses four different fact-dependent approaches to deciding Fourth Amendment claims in the criminal context).

154 *See* California v. Greenwood, 486 U.S. 35, 37 (1988).

bution of his or her information.[155] This voluntary consent rationale is consistent with the principle that consent to a search renders the search reasonable without probable cause or a warrant.[156] However, the seminal cases that rely on consent to justify a warrantless search involve a defendant who expressly agreed to the search in person.[157] Indeed, *Georgia v. Randolph* suggests that a third party cannot consent to a search on behalf of a spouse who is also present in the home.[158] The third-party doctrine departs from the cases of actual consent by implying consent where it has not in fact been given. This looks more like constructive consent than voluntary consent, although the Supreme Court has not explicitly adopted a theory of constructive consent.[159]

Justice Antonin Scalia argued, in dissent, that a hospital is free to voluntarily report the results of a patient's diagnostic tests to the police, because reporting by the hospital is consensual and therefore not a Fourth Amendment violation.[160] Under this view, it is the consent of the third party, not of the patient, that controls.[161] Justice Scalia concludes that "information obtained through violation of a relationship of trust is obtained consensually, and is hence not a

---

155 This is the reasoning seen in the false friend cases. *See, e.g.*, United States v. White, 401 U.S. 745, 751 (1971); Hoffa v. United States, 385 U.S. 293, 293 (1966) (quoting Lopez v. United States, 373 U.S. 427, 465 (1963) (Brennan, J., dissenting)).

156 *See* Sherry F. Colb, *What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 STAN. L. REV. 119, 123 (2002) (arguing that many third-party doctrine cases should be reevaluated under consent principles); Christine Jolls, *Privacy and Consent Over Time: The Role of Agreement in Fourth Amendment Analysis*, 54 WM. & MARY L. REV. 1693, 1694 (2013) (describing when and how consent to searches has been determinative); Kerr, *supra* note 102, at 589–90 (arguing that third-party doctrine cases are better viewed as cases of consent to disclosure rather than abandonment of privacy expectations).

157 *See, e.g.*, Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973) (concerning an in-person consent to search of a car).

158 Georgia v. Randolph, 547 U.S. 103, 112 (2006). *But see* Fernandez v. California, 134 S. Ct. 1126, 1129 (2014) (finding that once the objecting occupant is removed from the premises, a third party can consent to a search).

159 *See* Jolls, *supra* note 156, at 1701 (arguing that the validity of consent could vary depending on whether the search is contemporaneous with or much later than the consent). Cases involving drug testing of government employees have not relied on express, contemporaneous consent by individual employees. Instead, their "consent" to testing was a condition of their employment. *See* Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656, 672 (1989) (upholding drug testing of applicants for U.S. Custom Service jobs involving drug interdiction or carrying a firearm); *see also infra* Part IV.

160 Ferguson v. City of Charleston, 532 U.S. 67, 96 (2001) (Scalia, J., dissenting).

161 *Schneckloth*, 412 U.S. at 248 (stating that a search with consent does not violate the Fourth Amendment).

search."[162] As precedent for this conclusion, however, Justice Scalia relies on criminal cases in which a criminal suspect or defendant has confided something about a crime to an informant, and the informant passes the information on to law enforcement.[163] While the defendant may have hoped or even expected the informer would not betray the confidence, the informant had no duty of confidentiality to the defendant. Those facts differ from a patient's justifiable reliance on a health provider's duty to keep medical information confidential.[164] More importantly, a provider who is compelled by law to report patient data to a government agency does not voluntarily consent to disclose the information.[165] Thus, the false friend and willing informant cases offer no precedent for the notion that providers consent to disclosing data pursuant to mandatory reporting laws.

The abandonment/consent rationale has lost most of its credibility in today's interdependent economy. Only those living "off the grid" can avoid providing detailed personal information to accomplish the most basic tasks of daily living.[166] Bank, telephone, cable, internet, insurance, employment, household purchases, and most other ordinary transactions require entrusting third parties with detailed personal information.[167] The information is often particularly sensi-

---

162 *See Ferguson*, 532 U.S. at 96 (Scalia, J., dissenting) (explaining how information obtained through a violation of trust is consensual and thus does not trigger a Fourth Amendment violation).

163 *See, e.g.*, United States v. White, 401 U.S. 745, 746–47 (1971); Hoffa v. United States, 385 U.S. 293, 311 (1966); United States v. Dunning, 312 F.3d 528, 531 (1st Cir. 2002) (holding that a prison inmate had no reasonable expectation of privacy in letters sent to girlfriend).

164 Fort Wayne Women's Health v. Bd. of Commissioners, Allen Cty., Indiana, 735 F. Supp. 2d 1045, 1057 (N.D. Ind. 2010); Alberts v. Devine, 479 N.E.2d 113, 118 (Mass. 1985).

165 *See* Carroll v. City of Westminster, 233 F.3d 208, 210 (4th Cir. 2000) (drug testing); Aubrey v. Sch. Bd. of Lafayette Parish, 148 F.3d 559, 562 (5th Cir. 1998) (drug testing); Nat'l Fed'n of Fed. Emps. v. Weinberger, 818 F.2d 935, 943 (D.C. Cir. 1987) (stating that "a search [drug testing] otherwise unreasonable [under the Fourth Amendment] cannot be redeemed by a public employer's exaction of a 'consent' to the search as a condition of employment"); McDonell v. Hunter, 809 F.2d 1302, 1310 (8th Cir. 1987) (drug testing); *see also* Pauline T. Kim, *Privacy Rights, Public Policy, and the Employment Relationship*, 57 OHIO ST. L.J. 671, 701 (1996) (arguing for use of the special needs doctrine for routine investigations in the employment context); Paul M. Secunda, *Privatizing Workplace Privacy*, 88 NOTRE DAME L. REV. 277, 282 (2012) (arguing for using the special needs doctrine for routine suspicionless investigations and probable cause for individual investigations of wrongdoing).

166 *See* Posner, *supra* note 30, at 248 ("[A] person would have to be a hermit to be able to function in our society without voluntarily disclosing a vast amount of personal information to a vast array of public and private demanders."); *see also supra* note 109.

167 Laura Donahue, *Bulk Data Collection: Statutory and Constitutional Considerations*, 37 HARV. J.L. & PUB. POL'Y 757, 870 (2014) (stating that "[t]he extent to which we rely on electronic communications to conduct our daily lives is of a fundamentally different scale and

tive in the context of the physician-patient relationship. Thus, the idea that disclosure is voluntary or that it equates to consent to further disclosure or to granting a third party control over the information seems implausibly archaic.[168] Rather, applying the third-party doctrine to obtain information that a person cannot realistically avoid giving third parties is functionally the same as allowing the government to seize the information directly from the person.[169]

The Supreme Court's decisions in *Riley v. California*[170] and *United States v. Jones*[171] suggest some support for this conclusion. Justice Sotomayor, in an often-quoted concurrence in *Jones*, noted:

> [I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. . . . I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.[172]

The unanimous decision in *Riley* took this sentiment to heart, recognizing that digital technology and information pose new challenges to Fourth Amendment doctrines. The Court concluded that the police needed a warrant to search the arrested suspect's smart phone, because the phone's contents could not be considered part of an otherwise permissible warrantless search incident to an arrest.[173] Chief Justice Roberts' opinion rejected the government's argument that searching a cell phone was materially indistinguishable from searching physical items:

> That is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point

---

complexity than the situation that existed at the time the Court heard arguments in *Smith*").

168 See Kiel Brennan-Marquez, *Fourth Amendment Fiduciaries*, 84 FORDHAM L. REV. 611, 638, 647 (2015) (arguing that "sharing information with a doctor is the precondition of obtaining medical care," rendering such sharing involuntary).

169 Donald A. Dripps, *Perspectives on the Fourth Amendment*, MINN. L. REV., manuscript at 24 (forthcoming 2015), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2692296 ("To the extent that the consumer has no way to opt-out of sharing with the government what she shares with the provider, the data collected are indistinguishable from the government acquiring . . . data directly.").

170 *See* Riley v. California, 134 S. Ct. 2473, 2497 (2014) (Alito, J., concurring).

171 United States v. Jones, 132 S. Ct. 945, 954 (2012).

172 *Id.* at 957 (Sotomayor, J., concurring).

173 The exigent circumstances exception to the warrant requirement was not at issue, because police searched the phone about two hours after taking Riley into custody. *See Riley*, 134 S. Ct. at 2480–81.

> B, but little else justifies lumping them together. Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse.[174]

The opinion described the vast amount of information that can be accessed through a cell phone, a description that also applies to any device that uses the internet, specifically noting that "a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house."[175] Among the sensitive information mentioned is health information:

> [C]ertain types of data are also qualitatively different. An Internet search and browsing history, for example, can be found on an Internet-enabled phone and could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD.[176]

Riley makes clear that the government may need some individualized suspicion to search the contents of a person's telephone, which is typically held remotely by third parties: "Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant."[177]

The *Riley* opinion thus suggests that the Court is beginning to recognize that the transformation wrought by information technology may require easing the categorical boundaries of Fourth Amendment doctrines. This may translate to the third-party doctrine.

A second reason for the third-party doctrine appears to be that the third party collects the information for its own use in its business.[178] Stated another way, the information about an individual becomes the property of the third party, who is free to dispose of the information as it pleases, like the bank in *Miller* or the telephone company in *Smith*. Even if one accepts this reasoning, it does not necessarily follow that the government is entitled to obtain the information without the consent of either the third party who holds the

---

174 *Id.* at 2488–89.

175 *Id.* at 2491. *Riley* can be viewed as a recognizing that the breadth of information uncovered or perused would grossly exceed the purposes for which a warrantless search incident to arrest is conducted (officer safety and spoliation of evidence) and therefore has constitutional significance. The sensitivity of the information may be of secondary importance, because the search of a wallet or purse incident to arrest can reveal equally sensitive information, such as a prescription bottle or an Alcoholics Anonymous thirty-day chip.

176 *Id.* at 2490.

177 *Id.* at 2495.

178 *See, e.g.*, Smith v. Maryland, 442 U.S. 735 (1979); United States v. Miller, 425 U.S. 435, 444 (1976); Couch v. United States, 409 U.S. 322, 327 (1973); *see also* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 101, 147–50 (2004).

information or the person who is the information source. Mandatory reporting laws do not allow the third party to refuse. Thus, by itself, the premise that the third party has custody or control over the information does not answer the question whether the government can compel the third party to turn it over.

Holders of medical information might be considered bailees, who hold the information for limited purposes and are not free to otherwise dispose of it without the source's permission.[179] So far, most cases have limited this concept of bailment to circumstances in which the bailor was not expected to keep the items for its own use.[180] Health providers do use a patient's information in their business, albeit for the patient's benefit. While medical records may facilitate the provider's treatment of patients, they are not created solely to manage business practices. Medical records contain information that a patient entrusts to her physician (or hospital or other provider) for specific, limited purposes.[181] The physician, who owes quasi-fiduciary duties to the patient, is often viewed as holding the contents of the patient's medical record as a custodian or possibly a type of trustee for the benefit of the patient.[182]

While physicians and health care facilities may have custody of medical records, they do not necessarily view themselves as owning the contents in the same fashion or to the same extent that banks own their business records of financial transactions. Scholarly views of medical record ownership vary, with some commentators arguing that while the provider may own the record, the patient owns the information in the record.[183] Others note that patients cannot assert any ownership interest in medical records or the information they contain.[184] And state laws vary in their attribution of ownership to the

---

179 *See* Henderson, *supra* note 146, at 437–38 (suggesting that the Fourth Amendment might protect data left with a bailee that is not for the bailee's own use).

180 *See, e.g.*, United States v. Most, 876 F.2d 191, 197 (D.C. Cir. 1989) (bag left with store clerk); United States v. Barry, 853 F.2d 1479, 1482 (8th Cir. 1988) (suitcase left at airport). *But see* United States v. Warshak, 631 F.3d 266, 282-83 (6th Cir. 2010) (email held by service provider).

181 *See* Canterbury v. Spence, 464 F.2d 772, 782 (D.C. Cir. 1972) ("The patient's reliance upon the physician is a trust of the kind which traditionally has exacted obligations beyond those associated with arms-length transactions.").

182 Principles of medical ethics confirm the physician's duty of confidentiality. AMA, Principles of Medical Ethics, www.ama-assn.org/ama/pub/physician-resources/medical-ethics/code-medical-ethics/principles-medical-ethics.page ("IV. A physician shall . . . safeguard patient confidences and privacy within the constraints of the law.").

183 *See* GEORGE J. ANNAS, THE RIGHTS OF PATIENTS 227 (Eve Carey, ed., 3d ed. 2004).

184 *See, e.g.*, Barbara Evans, *Much Ado About Data Ownership*, 25 HARV. J.L. & TECH. 70, 74–75 (2011); Hoffman & Podgurski, *supra* note 1 at 111.

patient or the provider, with many not expressly addressing the issue.[185] In these circumstances, one cannot confidently conclude that the information in medical records is indisputably the property of the third party to do with as it chooses.

Indeed, Professor Jack Balkin argues that professionals like physicians qualify as "information fiduciaries" who must not breach confidentiality without the patient's consent or a very strong reason.[186] Kiel Brennan-Marquez argues that such information fiduciaries acquire obligations not because they are trusted in fact, but because they perform an important social function that requires information sharing.[187] The fiduciary duties of care and loyalty—and confidentiality—are normative constraints intended to prevent exploitation of the more vulnerable party by the more powerful party in an arm's length relationship.[188]

There is a strong ethical tradition in medicine, codified in statutes and case law, of keeping patient information confidential.[189] Of course, common law duties of confidentiality themselves do not give rise to constitutional protection. After all, *Miller* did not consider that common law recognition of a confidential relationship between a bank and a depositor affected the depositor's expectation of privacy.[190] Congress reacted to *Miller* by enacting the Right to Financial Privacy Act of 1978 to permit bank customers to challenge the government's justification for subpoenas of bank records.[191] Unlike the Court, Congress at least recognized that people do have some reasonable expectation of privacy in their financial information, even if government sometimes has good reason to override that expectation.

---

185 *Cf.* FLA. STAT. § 456.057 (1) ("[T]he term "records owner" means any health care practitioner who generates a medical record after making a physical or mental examination of, or administering treatment or dispensing legend drugs to, any person."); MASS. GEN. LAWS ANN. ch. 111, § 70 (2015) (implying that clinics and identified heath facilities own the records because the obligations to maintain them transfer with a change in ownership of the facilities themselves); VA. CODE ANN. § 32.1-127.1:03(A) (2015) ("Health records are the property of the health care entity maintaining them. . . .").

186 Jack Balkin, *Information Fiduciaries in the Digital Age*, BALKINIZATION (Mar. 5, 2014), http://balkin.blogspot.com/2014/03/information-fiduciaries-in-digital-age.html.

187 Brennan–Marquez, *supra* note 168, at 613, 628 (arguing that the concept of misplaced trust should not apply to information fiduciaries like hospitals and physicians).

188 *Id.* at 649–51.

189 *See, e.g.*, AMA, Principles of Medical Ethics, *supra* note 182; Alberts v. Devine, 479 N.E.2d 113, 118–20 (Mass. 1985) .

190 *See* Peterson v. Idaho First Nat'l Bank, 367 P.2d 284 (Idaho 1961) (concerning breach of duty of confidentiality by bank); Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 133 (2007) (comparing U.S. and British tort law governing breach of confidentiality).

191 12 U.S.C. §§ 3401–21.

The question is whether all privacy protection for records held by third parties must come from the legislature and none from the Fourth Amendment.[192]

A third rationale for the third-party doctrine is that the person has no reasonable expectation of privacy in the information. This reason has at least two different interpretations. One is essentially the same as voluntary abandonment or consent and is unpersuasive for the same reasons. The second is that the information at issue is not something that society is prepared to recognize as worth protecting. Or, in *Katz* terminology, the expectation is not "one that society is prepared to recognize as 'reasonable.'"[193] This reason has more bite, but is fact-dependent. As noted above, there are enough laws limiting the disclosure of health information to conclude that society accepts as reasonable an expectation of privacy in that information. Such laws recognize that it is the content of the information that determines whether it is worthy of expectations of privacy, not who holds it.[194] Society may recognize some information as warranting privacy protection, regardless of where it sits.

In *Ferguson v. City of Charleston*, the Supreme Court recognized that patients have a reasonable expectation that the information they provide to their physicians will be used solely for the purpose of their own diagnosis and treatment and not shared with other entities without the patient's consent—at least for law enforcement purposes.[195] The state hospital in *Ferguson* tested urine samples from pregnant women in prenatal care or at delivery to identify cocaine users and reported those with positive tests to police, all without a warrant, probable cause, individualized suspicion or (the Court assumed) the patients' knowledge or consent.[196] The police initially arrested all re-

192 *See* Charles E. MacLean, Katz *on a Hot Tin Roof: The Reasonable Expectation of Privacy Is Rudderless in the Digital Age Unless Congress Continually Resets the Privacy Bar*, 24 ALB. L.J. SCI. & TECH. 47, 76 (2014) (arguing that Congress should periodically amend laws like the ECPA and SCA to protect digital privacy, thereby establishing a floor of reasonable expectations of privacy).

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

194 *But see* Brennan–Marquez, *supra* note 168, at 639–40 (arguing against focusing on the sensitivity of the information, rather than the fiduciary duties of the holder).

195 Ferguson v. City of Charleston, 532 U.S. 67, 78 (2001).

196 Patients were selected for testing if they met at least one of the following nine criteria: no, late, or incomplete prenatal care; abruption placentae; intrauterine fetal death; preterm labor or intrauterine growth retardation "of no obvious cause"; previously known drug or alcohol abuse; or unexplained congenital anomalies. *Ferguson*, 532 U.S. at 70–73. These factors, however, could be present for many reasons unrelated to drug use. *See id.* at 76; Emmalee S. Bandstra et al., *Prenatal Drug Exposure: Infant and Toddler Outcomes*, 29 J. ADDICTIVE DISEASES 245 (2010); Jeanne Flavin & Lynn M. Paltrow, *Punishing Pregnant*

ported patients on drug charges. Later, under a modified policy, only patients who failed to enter and comply with a drug treatment program were arrested. The hospital argued that its search and reporting policy was justified by the special need to protect the health of both mother and child.[197] The Court rejected that claim, finding that the "Fourth Amendment's general prohibition against nonconsensual, warrantless, and suspicionless searches necessarily applies to such a policy."[198]

A threshold question was whether the patients had consented to providing a urine sample for the purpose of drug testing and reporting test results to law enforcement.[199] The Supreme Court majority presumed lack of consent, and on remand to decide that issue, the Fourth Circuit Court of Appeals held that there was insufficient evidence that any patient "validly consented to the taking and testing of her urine *for law enforcement, as opposed to medical, purposes*".[200] Since the Supreme Court's decision rested heavily on the law enforcement purpose of the drug tests, the patients' lack of consent cemented the conclusion that the search violated the Fourth Amendment.

Ferguson did not address the question whether police could compel the hospital to produce the drug test results if there had been no policy in effect and physicians had ordered the tests solely for purposes of treating the women. The Court did not mention the third-party doctrine. It analyzed the case in terms of the special needs doctrine, finding that law enforcement is not a special need that would justify an exception to the warrant requirement. But, in doing so, it made clear that the patients had a reasonable expectation of privacy in their medical information:

> The reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with non-medical personnel without her consent.[201]

Drug-Using Women: Defying Law, Medicine, and Common Sense, 29 J. ADDICTIVE DISEASES 231, 233 (2010); Barry Zuckerman, *Drug-Exposed Infants: Understanding the Medical Risks*, 1 THE FUTURE OF CHILDREN 26, 28–31 (1991). The vast majority tested were poor women of color. Dorothy Roberts, *Punishing Drug Addicts Who Have Babies: Women of Color, Equality, and the Right of Privacy*, 104 HARV. L. REV. 1419, 1421 (1991).

197 *Ferguson*, 532 U.S. at 81. For further discussion of the special needs doctrine, *see infra* Part V.

198 *Ferguson*, 532 U.S. at 86 (Kennedy, J., concurring). The urine tests were "indisputably searches within the meaning of the Fourth Amendment." *Id.* at 76.

199 The Court was not entirely clear whether it was addressing consent to (1) taking the sample, (2) testing the sample for cocaine, or (3) reporting the results to law enforcement, but appeared to be particularly concerned about (3). *See id.* at 77–80.

200 Ferguson v. City of Charleston, 308 F.3d 380, 395 (4th Cir. 2002) (emphasis in original).

201 *Ferguson*, 532 U.S. at 78.

The implication is that law enforcement would need a warrant, or at least a subpoena, to obtain the drug test results. In this case, however, the police had no *a priori* reason to suspect any of the patients of a crime.[202]

Nevertheless, one might ask why the Court did not consider the third-party doctrine. In theory, that doctrine would allow the hospital to give medical test results to the police voluntarily, leaving the patients with no Fourth Amendment protection. Indeed, this is what Justice Scalia argued, dissenting from the *Ferguson* majority's opinion.[203] In the dissent's view, if a patient consents to a medical test in course of ordinary treatment, she loses any expectation of privacy in the results of that test.

What might *Ferguson* imply for mandatory reporting laws requiring test results or other medical information to be reported to a government agency? The dissent argued that the majority's opinion would mean that "the Fourth Amendment would invalidate those many state laws that require physicians to report gunshot wounds, evidence of spousal abuse, and . . . evidence of child abuse."[204] In a footnote, the dissent adds, "If voluntary betrayal of a trust in mere cooperation with the police constitutes a Fourth Amendment search, surely betrayal of a trust at the direction of the legislature must be."[205] Justice Anthony Kennedy, concurring in the majority's opinion, disagreed, noting without explanation that the decision "does not call into question the validity of mandatory reporting laws such as child abuse laws which require teachers to report evidence of child abuse to the proper authorities, even if arrest and prosecution is the likely result."[206] These brief comments cannot be said to resolve the question.

None of the Justices' opinions actually analyzes mandatory reporting laws, of course. State reporting laws are enacted in order to permit health care providers to violate their duty of confidentiality by disclosing patient information. If there is no constitutional impediment to voluntary reporting by providers, why do states bother to enact such laws? One answer may be that providers desire statutory confirmation that they will not be subject to liability to patients for such disclosures. If true, it turns reporting laws into symbolic gestures. Legislatures do sometimes grant immunity from liability to

202 *See supra* note 186.

203 *Ferguson*, 532 U.S. at 96 (Scalia, J., dissenting); *see also supra* text accompanying notes 123–26.

204 *Ferguson*, 532 U.S. at 97 (Scalia, J., dissenting).

205 *Id.* at 96 n.3.

206 *Id.* at 90 (Kennedy, J., concurring).

those entities who comply with regulations that the state is empowered to adopt.[207] But, such legislation is not required. Why, then, would states presume that they must enact affirmative legislation to justify the compelled reporting of medical information? The Court's decisions applying the third-party doctrine do not offer a clear answer.

It is possible that the third-party doctrine could be extended to compel third party reporting on an ongoing basis without individualized suspicion.[208] It is also possible that the third-party doctrine should not apply to those circumstances at all, either because it has no application in the civil context or because other Fourth Amendment doctrines are better suited to resolving that issue. Both the line of cases involving administrative searches and that involving suspicionless searches for purposes of 'special needs' beyond law enforcement address the application of the Fourth Amendment in the civil context. To those cases, we now turn.

IV. ADMINISTRATIVE SEARCHES

The line of cases developing the special needs doctrine grew alongside the cases addressing administrative searches, such that the special needs doctrine includes elements of the administrative search exception plus its own increasingly opaque boundaries. It is worth considering administrative searches themselves, since reporting laws could be seen as a form of searching the records of health entities.

Administrative searches conducted without probable cause were initially justified as a narrow exception to Fourth Amendment requirements.[209] The exception applied first to inspections of regulated business premises and housing. Routine inspections for compliance with health and safety regulations were believed necessary to identify and prevent hidden dangers, such as defective heating or electrical systems, but government typically had no probable cause to suspect

---

207 Good Samaritan Laws often offer protections from liability for classes of identified individuals (usually medical professionals) for unintended harms caused by the use of their skills to provide aid, usually in an emergency outside their practice. For a listing of state laws, see Suzanne E. Turner, *Good Samaritan Laws: A Comparative Study of Laws That Protect First Responders Who Assist Accident Victims*, A RESEARCH NOTE BY DECHERT LLP FOR SAVELIFE FOUNDATION (May 2014), http://www.trust.org/contentAsset/raw-data/7be34cce-ea0d-4c90-8b39-53427acf4c43/file.

208 The Fourth Amendment "generally bars officials from undertaking a search or seizure absent individualized suspicion." Chandler v. Miller, 520 U.S. 305, 308 (1997).

209 LAFAVE, *supra* note 102, §§ 10.1–10.2; *see also* Los Angeles v. Patel, 135 S. Ct. 2443, 2457 (2015) ("To classify hotels as pervasively regulated would permit what has always been a narrow exception to swallow the rule.").

that any particular person or business was violating the law.[210] Dangerous conditions that needed remediation were not necessarily apparent, so neither probable cause nor location-specific suspicion could be expected.[211] To prevent arbitrary or abusive searches, a search warrant was required to describe the type of business or geographic area to be searched.[212] Instead of basing warrants on probable cause, however, a court could determine whether government has "a valid public interest [that] justifies the intrusion contemplated."[213]

As the scope of business regulation expanded, licensing and similar legislation included requirements for when and how such routine inspections took place.[214] These requirements became an accepted substitute for the warrant requirement as a check on arbitrary government action.[215] The Court summarized the criteria for a permissible warrantless search as follows: (1) the regulatory scheme furthers a "substantial" government interest; (2) the warrantless inspections are "necessary to further [the] regulatory scheme"; and (3) the "inspection program, in terms of certainty and regularity of its application," is a "constitutionally adequate substitute for a warrant."[216]

Still, warrantless administrative searches were limited to searches that were not looking for evidence of a crime,[217] were conducted pur-

---

210 See v. City of Seattle, 387 U.S. 541, 545 (1967) (striking down fire code inspections, but indicating that warrants for future inspections could be issued pursuant to a more flexible standard for probable cause to enforce regulations).

211 *See, e.g.*, New York v. Burger, 482 U.S. 691 (1987) (auto disassembly business); Marshall v. Barlow's, Inc., 436 U.S. 307 (1978) (electrical and plumbing installation); United States v. Biswell, 406 U.S. 311 (1972) (licensed pawn shop and firearms dealer); Colonnade Catering Corp. v. United States, 397 U.S. 72 (1970) (licensed liquor store).

212 Camara v. Municipal Court of S.F., 387 U.S. 523 (1967) (holding that annual inspection for housing code violations required a warrant, but warrant could be based on likelihood of finding violations in a geographic area instead of individualized suspicion). A warrant could encompass an entire geographic area or an industry within that area, because officials need to know whether that regulated population is complying with health, safety, fire and sanitation requirements. *Id.* at 538.

213 *Id.* at 539.

214 *See id.* at 528 ("The basic purpose of this Amendment . . . is to safeguard the privacy and security of individuals against arbitrary invasions by government officials.").

215 *See* Eve Brensike Primus, *Disentangling Administrative Searches*, 111 COLUM. L. REV. 255, 262–70 (2011) (describing the development of administrative search doctrine).

216 *Burger*, 482 U.S. at 702–03 (citation omitted). The second criterion allows warrantless inspections where advance notice would allow violations to be concealed or eliminated. *Biswell*, 406 U.S. at 316; *see*, 387 U.S. at 545.

217 *See, e.g.*, United States v. Ortiz, 422 U.S. 891 (1975) (striking down checkpoint to search vehicles for illegal aliens). The distinction between civil and criminal searches is not always as clear as the doctrine suggests, because criminal sanctions such as fines and incarceration are often authorized and imposed for refusing a search or for violations found as a result of an inspection. *Camara*, 387 U.S. at 531.

suant to statutory rules that limited official discretion,[218] did not suspect or target individuals, and where the intrusion on privacy was minimal and not personal.[219] As government found more reasons to look for problems, the focus of analysis shifted from the earlier goal of ensuring safe premises to the reasonableness of the government's purpose in obtaining certain information and the procedural regularity of the search process.[220] Thus, the government's reason for conducting inspections without any prior suspicion of individualized wrongdoing assumed increasing salience in doctrinal analysis, overshadowing concern for intrusions on personal privacy.

Many decisions do permit administrative subpoenas in the civil regulatory context to investigate threats to employee health and safety. These decisions fit within the original conception of administrative searches—enforcement of civil regulatory requirements pursuant to express procedural requirements. For example, the Mine Safety Health Administration's interest in the health and safety of miners outweighed the miners' interest in keeping their medical information out of the wrong hands in *Big Ridge, Inc. v. Federal Mine Safety and Health Review Commission.*[221] Mine Safety Health Administration ("MSHA") regulations required mine operators to allow inspectors to obtain medical and personnel records to verify the validity of the operator's reports on injuries to miners. In this case, MSHA sought the records without a warrant to see whether an operator with many past violations was underreporting injuries.

The court noted that *United States v. Miller* might be thought to preclude any Fourth Amendment right to privacy on the part of the miners, because the records were in the custody of the mine operator.[222] But it also found that "some personal records are so private that, even when entrusted to another, an individual retains some

218 Donovan v. Dewey, 452 U.S. 594, 605 (1981).

219 Where a search could be based on individualized suspicion, however, probable cause or a warrant was often required. *See, e.g.*, Delaware v. Prouse, 440 U.S. 648, 659 (1979) (rejecting random vehicle stops to find unlicensed drivers in favor of targeting vehicles in violation of motor vehicle laws).

220 The *Camara* Court recognized that a warrant for an administrative search could not be based on probable cause for finding individual violators. Instead, a warrant could encompass an entire geographic area or an industry within that area, because officials need to know whether that entire population is complying with health, safety, fire and sanitation requirements. *Camara*, 387 U.S. at 535; *see also* Tracey Maclin, *The Central Meaning of the Fourth Amendment*, 35 WM. & MARY L. REV. 197, 198–200 (1993); Scott E. Sundby, *A Return to Fourth Amendment Basics: Undoing the Mischief of* Camara *and* Terry, 72 MINN. L. REV. 383, 383–86 (1988).

221 715 F.3d 631, 644 (7th Cir. 2013).

222 *Id.* at 649.

amount of protection of the privacy of the records in the third party's custody."[223] This presented "a difficult question of balancing" for the court.[224] It found that the demands for records were best understood as administrative subpoenas, rather than warrantless searches. They were justified without a warrant because the record request was necessary to protect the workers, it met the administrative search criteria of *Burger*, and MSHA was legally required to keep miners' medical information confidential.[225]

Earlier, in *United States v. Westinghouse Electric Corp.*, the National Institute for Occupational Safety and Health ("NIOSH") received a request from an employee union to conduct a "health hazard evaluation" at a Westinghouse plant.[226] After inspecting the facility, NIOSH issued a subpoena to obtain employee medical records to determine whether employees were experiencing allergic reactions to hexahydrophthalic anhydride ("HHPA"). The circuit court found that the employees' medical records were entitled to privacy protection under the Fifth Amendment Due Process Clause, without discussing the Fourth Amendment.[227] But it concluded that the employees' privacy interests were outweighed by a combination of factors: the agency's interest in protecting occupational safety and health; its need for the records in order to compare employees' medical conditions before and after exposure to HHPA; the information was not highly sensitive, consisting primarily of routine test results; and NIOSH procedures for keeping the data secure and confidential. Thus, the court issued an order enforcing the subpoena, but nonetheless allowed each employee to object to the production of his or her own records.[228] This result may have been influenced by the fact

223 *Id.*

224 *Id.*

225 *Id.* at 650 (describing how the federal Privacy Act, 5 U.S.C. § 552a, required the agency to keep the employees' personal information confidential and not disclose it to others without the employee's consent). In addition, the federal Mine Safety and Health Act allowed the mine operators to contest proposed penalties for noncompliance, which the operator did in this case. *Id.* at 652.

226 638 F.2d 570, 572 (3d Cir. 1980).

227 *Id.* at 581 n.7 ("[T]he best solution-no matter who may be the custodian of the records in the particular instance-is to require that the party seeking to secure the records by subpoena give the patient notice of the issuance of the subpoena, and to permit the patient to contest its enforcement by whatever means is regarded as satisfying the requirements of due process." (citing Kaiser, Privacy and Medical Record-Keeping, included in Privacy: the Collection, Use, and Computerization of Personal Data (Part 2): Joint Senate Hearings before the Ad Hoc Comm. on Government Operations and Subcomm. on Constitutional Rights of the Comm. of the Judiciary, 93rd Cong., 2d Sess. 2240, 2246 (June 18–20, 1974))).

228 *Westinghouse Elec. Corp.*, 638 F.2d at 578–80.

NIOSH's investigation was initiated in response to a request on behalf of the employees themselves.

These and similar administrative searches of employee medical records have one similarity to reporting laws intended to investigate contagious disease outbreaks: the agencies are looking for existing threats to the health or safety of a particular group of people – threats that can be removed and that the agency is authorized to halt. The agency may need identifiable information about certain individuals and their current medical status in order to find and stop the spread of disease.

Yet the administrative subpoena cases also differ from other medical reporting or surveillance systems, like PDMPs, newborn screening banks, and registries of immunizations, cancer and other chronic diseases. The latter are not designed to identify immediate threats to the health or safety of a particular group of people. Rather, they engage in the ongoing collection of data for the purpose of making it available for multiple future uses – primarily civil, but occasionally criminal. Thus, these cases offer rather strained analogies for determining the validity of most health surveillance laws.

In 2015, a bare 5-4 majority of the Court constrained the scope of administrative searches in a case where the government's reason was not questioned. In *Los Angeles v. Patel*, it concluded that the administrative search exception applies only to closely regulated businesses – those that are comprehensively regulated and inherently "pose a clear and significant risk to the public welfare," and hotels did not fall into this category.[229] Hotel operators successfully challenged a 116-year-old city ordinance requiring them to record identifying information about guests and allow police to inspect the guest registers on demand. Noncompliance was a misdemeanor. The Court held that its prior decisions required the subject of an administrative search to have an "opportunity to obtain precompliance review before a neutral decisionmaker."[230] This would allow administrative subpoenas,

229 Los Angeles v. Patel, 135 S. Ct. 2443, 2454 (2015). The Court said that "searches conducted outside the judicial process, without prior approval by [a] judge or [a] magistrate [judge], are per se unreasonable . . . subject only to a few specifically established and well-delineated exceptions." *Id.* at 2452 (internal quotation marks omitted). It further noted that it had recognized only four such industries in past decisions. *Id.* at 2454 (citing New York v. Burger, 482 U.S. 691 (1987) (automobile junkyard); Donovan v. Dewey, 452 U.S. 594 (1981) (mining); United States v. Biswell, 406 U.S. 311, 315 (1972) (firearms dealers); Colonnade Catering Corp. v. United States, 7 U.S. 72, 76–77 (1970) (liquor sales)).

230 *Id.* at 2452.

but also permit the subject of the subpoena to seek an order to quash.[231]

Patel is a narrow, but significant, ruling. The majority assumed that the searches authorized by the ordinance "serve a special need other than conducting criminal investigations: They ensure compliance with the recordkeeping requirement, which in turn deters criminals from operating on the hotel's premises."[232] Nevertheless, the Court also noted in a footnote that the law was facially unconstitutional, even if the search's purpose were to facilitate criminal investigations.[233] In particular, it emphasized that closely regulated industries are the exception, not the rule.[234] Laws merely requiring a license and adherence to sanitary standards are not enough to qualify.[235] The dissenting Justices disagreed with this analysis, finding the city ordinance "eminently reasonable"[236] and meeting the *Burger* standards.[237] Thus, the Court seems divided on how to define permissible, suspicionless administrative searches.

Should health care providers, pharmacies, or insurers be considered closely regulated industries for purposes of permitting mandatory reporting? These entities certainly have a health and safety mission, but it is not clear whether the Supreme Court would characterize them as closely regulated for purposes of the administrative search exception to the Fourth Amendment.[238] One obstacle to analogizing reporting laws to administrative searches is that reporting laws (in contrast to licensure laws) lack the administrative regulatory structures authorizing and constraining agency investigations of an industry. That is, the reporting statutes do not typically include *Burger* standards regulating access to medical records. If government

231 *Id.* at 2452–53 ("Absent an opportunity for precompliance review, the ordinance creates an intolerable risk that searches authorized by it will exceed statutory limits, or be used as a pretext to harass hotel operators and their guests.").

232 *Id.* at 2452 (noting that the hotels did not challenge the requirement to keep a guest registry or the legitimacy of the city's interest, especially in preventing human trafficking).

233 *Id.* at 2452 n.2.

234 *Id.* at 2455; *see also* Free Speech Coal., Inc. v. Att'y Gen. U.S., 787 F.3d 142 (3d Cir. 2015) (striking down warrantless search of records kept by sexually explicit film producers as violation of Fourth Amendment). In *Free Speech Coalition, Inc.*, the court found that because this was not an administrative search of a closely regulated industry and there was no real risk of hiding or destroying records of actors' ages, a warrant would be needed to search records. *Id.* at 171–72.

235 *Patel*, 135 S. Ct. at 2455.

236 *Id.* at 2457 (Scalia, J., dissenting).

237 *Id.* at 2459.

238 *See, e.g.*, Williams v. Kentucky, 213 S.W.3d 671, 678 (Ky. 2006) (finding that a "warrantless raid" on a medical clinic to find evidence of unlawful physician prescriptions of controlled substances was not an administrative search of a closely regulated industry).

could require specific data to be reported simply as part of an administrative search, it should also be able to require access to the complete medical records of the facility. *Patel* suggests that there must be more justification than this.

Other federal and state court decisions support the conclusion that patients have a reasonable expectation of privacy in their medical records.[239] These cases typically require probable cause for a warrant or court order to obtain medical records for a criminal investigation or to enforce an administrative subpoena.[240]

An interesting example is *Tucson Woman's Clinic v. Eden*.[241] There, physicians who provide abortion services challenged the state's law requiring them, *inter alia*, to submit to warrantless inspections of their offices and provide unredacted patient medical records and send ultrasound prints to third parties.[242] The circuit court noted that the reason for allowing warrantless administrative searches for regulatory purposes is that closely regulated enterprises have a diminished expectation of privacy.[243] In contrast, it found, "the expectation of privacy is *heightened*" in abortion clinics.[244] This heightened expectation

239 *See* Doe v. Broderick, 225 F.3d 440, 450–51 (4th Cir. 2000) (noting that society recognizes as objectively reasonable a patient's expectation of privacy in records and files of his treatment maintained by substance abuse treatment center, because "medical treatment records contain intimate and private details that people do not wish to have disclosed, expect will remain private, and, as a result, believe are entitled to some measure of protection from unfettered access by government officials"); United States v. Westinghouse Elec. Corp., 638 F.2d 570, 577 (3d Cir. 1980) ("There can be no question that an employee's medical records, which may contain intimate facts of a personal nature, are well within the ambit of materials entitled to privacy protection. Information about one's body and state of health is matter which the individual is ordinarily entitled to retain within the 'private enclave where he may lead a private life.'"); State v. Skinner, 10 So. 3d 1212, 1218 (La. 2009) ("[W]e find that the right to privacy in one's medical and prescription records is an expectation of privacy that society is prepared to recognize as reasonable."); King v. State, 535 S.E.2d 492, 495 (Ga. 2000) ("[A] patient's medical information, as reflected in the records maintained by his or her medical providers, is certainly a matter which a reasonable person would consider to be private."); Commonwealth v. Riedel, 651 A.2d 135, 139–40 (Pa. 1994) (noting that a person has "a reasonable expectation of privacy in his medical records").

240 *See Skinner*, 10 So. 3d at 1218 ("[A]bsent the narrowly drawn exceptions permitting warrantless searches, we hold a warrant is required to conduct an investigatory search of medical and/or prescription records."); State v. Nelson, 941 P.2d 441, 449 (Mont. 1997) (finding the state must show probable cause for the issuance of an investigative subpoena for the discovery of medical records); *Riedel*, 651 A.2d at 139–40 (requiring probable cause for access to medical records); State v. Copeland, 680 S.W.2d 327, 330–31 (Mo. Ct. App. 1984) (requiring probable cause for the results of blood tests).

241 379 F.3d 531 (9th Cir. 2004).

242 *Id.* at 550 (emphasis in original).

243 *Id.*

244 *Id.* (emphasis in original).

arose not only because abortion is "a service grounded in a fundamental constitutional liberty," but also because "all provision of medical service in a private physicians' offices carries with it a high expectation of privacy for both physician and patient."[245] Thus, the court found that the clinics could not be considered closely regulated and the statute's authorization of warrantless searches violated the Fourth Amendment.[246]

V. SPECIAL NEEDS

The special needs exception to the warrant requirement extends the administrative search exception into the personal sphere, by permitting suspicionless searches of people, not just places.[247] Where government can demonstrate a "special need," searches of persons themselves, rather than places, have been held justifiable without individualized suspicion or a warrant.[248] The special needs line of cases represents a shift not merely in focus, but in doctrine.[249] Although the Court often asserts that "special needs" is a "closely guarded category of constitutionally permissible suspicionless searches,"[250] the cases make clear that suspicionless searches for special needs are no longer exceptional.

The Supreme Court's special needs cases most relevant here involve testing a group of individuals for illegal drugs.[251] The Court has upheld suspicionless drug testing when required pursuant to gov-

245 *Id.*

246 *Id.*

247 *See* City of Ontario v. Quon, 560 U.S. 746 (2010). Eve Brensike Primus traces the origins of the special needs doctrine from what she calls searches of "special subpopulations," and argues that initially, courts required some generalized suspicion that members of a subpopulation violated a civil requirement, such as a condition of employment or school attendance. Primus, *supra* note 215, at 260. She distinguishes this special needs doctrine from that originating in the cases addressing administrative or dragnet searches, and argues that courts have conflated the two lines of cases, creating doctrinal confusion and inappropriately expanding the rationale for suspicionless searches. *Id.* at 260–61.

248 This is a far cry from the principle stated in *Camara* that "except in certain carefully defined classes of cases, a search of private property without proper consent is 'unreasonable' unless it has been authorized by a valid search warrant." Camara v. Municipal Court of S.F., 387 U.S. 523, 528–29 (1967).

249 Primus, *supra* note 215, at 260.

250 *See, e.g.*, Chandler v. Miller, 520 U.S. 305, 309 (1997).

251 Drug tests typically entail providing a urine sample (sometimes collected under supervision) that is tested by a laboratory for the presence of specified illegal drugs, such as cocaine, heroin, marijuana, amphetamines, opiates, and barbiturates. Drug tests may also include breathalyzer tests and blood tests.

ernment regulation,[252] as a condition of government employment or promotion,[253] and participation in public school activities.[254] Initially, justification for testing was grounded in the fact that the persons tested were in safety sensitive positions, who could endanger the public if impaired by drug use. For example, in *Skinner v. Railway Labor Executives Ass'n*, federal regulations authorized drug testing of railroad employees after a serious accident, because impaired performance could cause injury to passengers.[255] Findings of a special need to protect public safety, however, have decayed from reasonable to barely plausible. In *Von Raab*, applicants for positions in the Customs Service were required to pass a drug test on the theory that those who used drugs could mishandle firearms or be subjected to bribery or extortion by drug dealers.[256] A majority of Justices found this "special need" sufficient, even though it was speculative and not based on any suspicion of members of the applicant pool.[257]

In *Vernonia School District 47J*, the Court's majority concluded that the school district demonstrated a special need to test students in athletic teams for drugs, because there were a few reports that athletes *might* have used marijuana and athletes were seen as role models for the rest of the student population.[258] In *Earls*, however, it upheld drug testing for students in school organizations like choir, band, Academic Team, Future Farmers, and Future Homemakers—groups that could hardly be classified as posing physical threats. *Earls* em-

252 *See, e.g.*, Skinner v. Ry. Labor Execs. Ass'n, 489 U.S. 602 (1989) (upholding drug testing of all railway employees involved in train accidents, when supervisors have evidence of drug or alcohol abuse among employees, and when links between impaired employees and accidents causing substantial personal injury and financial loss have been established).

253 *See, e.g.*, Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656 (1989) (upholding drug testing of applicants for U.S. Custom Service jobs involving drug interdiction or the carrying of a firearm).

254 Bd. of Educ. of Indep. Sch. Dist. No. 92 of Pottawatomie Cnty. v. Earls, 536 U.S. 822 (2002) (upholding drug testing of public school students who participate in any extracurricular school activity, including choir, band, academic teams, Future Farmers of America, and Future Homemakers of America); Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646 (1995) (upholding random drug testing of students in a public school's athletic teams, where there was some evidence of athletes leading a drug culture).

255 *Skinner*, 489 U.S. at 608–11.

256 *Id.* at 668–73 ("We think Customs employees who are directly involved in the interdiction of illegal drugs or who are required to carry firearms in the line of duty likewise have a diminished expectation of privacy in respect to the intrusions occasioned by a urine test.").

257 *Id.* at 669, 679.

258 *Vernonia Sch. Dist. 47J*, 515 U.S. at 662–65; *see also id.* at 649 ("The high school football and wrestling coach witnessed a severe sternum injury suffered by a wrestler, and various omissions of safety procedures and misexecutions by football players, all attributable in his belief to the effects of drug use.").

phasized that both decisions granted considerable leeway to school districts, based in part on their responsibility to protect the safety of students under their supervision.[259] In her dissenting opinion, Justice Ruth Bader Ginsburg challenged the factual basis for the majority's conclusion, saying:

> Notwithstanding nightmarish images of out-of-control flatware, livestock run amok, and colliding tubas disturbing the peace and quiet of Tecumseh, the great majority of students the School District seeks to test in truth are engaged in activities that are not safety sensitive to an unusual degree. There is a difference between imperfect tailoring and no tailoring at all.[260]

Nonetheless, the Court continues to insist that the special needs exception remains a "closely guarded category."[261] In *Chandler v. Miller*, the Court struck down a drug testing requirement for candidates for state political office, saying:

> Our precedents establish that the proffered special need for drug testing must be substantial—important enough to override the individual's acknowledged privacy interest, sufficiently vital to suppress the Fourth Amendment's normal requirement of individualized suspicion.[262]

The drug testing cases, however, do not offer persuasive reasons for finding a substantial need for testing high school band members, but not candidates for office. The risks these two groups pose, if any, are entirely different in scale.

Chief Justice William Rehnquist, dissenting in *Chandler*, disputed the notion that the special need must rise to the level of "important," arguing that any "proper governmental purpose other than law enforcement" would qualify as a special need.[263] *Vernonia* and *Earls* suggest that the special needs analysis has collapsed into a rational basis test, permitting suspicionless searches for almost any legitimate government purpose, other than law enforcement.[264]

---

259 *Id.*

260 *Earls*, 536 U.S. at 852 (Ginsburg, J., dissenting).

261 Chandler v. Miller, 520 U.S. 305, 309 (1997) ("Georgia's requirement that candidates for state office pass a drug test, we hold, does not fit within the closely guarded category of constitutionally permissible suspicionless searches."); *see also* City of Ontario v. Quon, 560 U.S. 746, 760–61 (2010); Arizona v. Gant, 556 U.S. 332, 338 (2009).

262 *Chandler*, 520 U.S. at 318. The offices included "Governor, Lieutenant Governor, Secretary of State, Attorney General, State School Superintendent, Commissioner of Insurance, Commissioner of Agriculture, Commissioner of Agriculture, Commissioner of Labor, Justices of the Supreme Court, Judges of the Court of Appeals, judges of the superior courts, district attorneys, members of the General Assembly, and members of the Public Service Commission." *Id.* at 309–10.

263 *Id.* at 325 (Rehnquist, C.J., dissenting).

264 *See generally* SLOBOGIN, *supra* note 41; Maclin, *supra* note 220.

Nevertheless, the Court has not expressly conflated its Fourth Amendment standards with minimum scrutiny under its due process standards of review. It continues to find that drug tests constitute searches when required by government. The question in these cases is whether the search was both substantively and procedurally reasonable when conducted without individualized suspicion or a warrant.[265] And the key factor in this line of cases has been the importance of the government's purpose for a suspicionless search—whether drug testing is warranted by a special need.[266]

In *Ferguson v. City of Charleston*, the Court found that the special need at issue must be the immediate purpose of the search, and not some speculative long-term goal that the search might help to achieve in the future.[267] The Court rejected, as overreaching, the hospital's argument that its goal was to help women and protect children:

> While the ultimate goal of the program may well have been to get the women in question into substance abuse treatment and off of drugs, the immediate objective of the searches was to generate evidence *for law enforcement purposes* in order to reach that goal. . . . Because law enforcement involvement always serves some broader social purpose or objective, under [hospital] respondent's view, virtually any nonconsensual suspicionless search could be immunized under the special needs doctrine by defining the search solely in terms of its ultimate, rather than immediate, purpose. Such an approach is inconsistent with the Fourth Amendment.[268]

Several possible conclusions may be drawn from *Ferguson*. The most obvious is that law enforcement does not qualify as a special need exception that excuses government from acting on individualized suspicion, probable cause, or a warrant.[269] A second possibility is that consent is necessary for a search that could reveal evidence of a crime and be reported to law enforcement. This brings us back to

---

265 The cases typically follow one of two paths from the Fourth Amendment's two clauses—those in which a warrantless search or seizure must be reasonable and those in which a warrant is required—although the reasoning in many cases appears somewhat overlapping or inconsistent. Whether the two clauses should legitimately be considered separately and how to interpret them remains debatable. *See generally* Solove, *supra* note 45.

266 *See, e.g.*, *Chandler*, 520 U.S. at 313–14.

267 Ferguson v. City of Charleston, 532 U.S. 67, 83–84 (2001).

268 *Id.* at 68, 84. The Court also rejected law enforcement purposes as a special need in *Indianapolis v. Edmond*, 531 U.S. 32 (2000) (overturning police program of suspicionless highway roadblocks to check vehicles for narcotics). In *Edmond*, the Court said that the possibility that the roadblocks might also serve a public safety purpose by getting drunk drivers off the road did not qualify as an independent special need that could justify a suspicionless search. *Id.* at 46.

269 *Ferguson*, 532 U.S. at 84 ("[T]his case simply does not fit within the closely guarded category of 'special needs.'").

the thorny question of whether consent to medical care is sufficient to allow a third party to report the results to the police, either voluntarily or under compulsion.[270] The Supreme Court assumed lack of consent to both testing and reporting.[271] The Fourth Circuit, on remand, found no consent to testing or reporting for law enforcement purposes, without addressing consent to testing for medical care.[272] Thus, the question remains somewhat unresolved. The case can then be seen as requiring consent to reporting only if the reports are intended for law enforcement. Would consent to reporting for a non-law-enforcement purpose be required in addition to consent for ordinary medical care? *Ferguson* offers a few hints, but no clear answer.

The Court distinguished the facts in *Ferguson* from its earlier drug testing cases, as follows:

> In the previous four cases, there was no misunderstanding about the purpose of the test or the potential use of the test results, and there were protections against the dissemination of the results to third parties. The use of an adverse test result to disqualify one from eligibility for a particular benefit, such as a promotion or an opportunity to participate in an extracurricular activity, involves a less serious intrusion on privacy than the unauthorized dissemination of such results to third parties. *The reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with nonmedical personnel without her consent.* In none of our prior cases was there any intrusion upon that kind of expectation.[273]

This language suggests that the Court saw a difference in kind between drug testing of employees and students, on one hand, and drug testing of patients in a medical care setting, on the other. More importantly, the Court seemed to link the testing with the reporting, saying that medical test results, even if part of the patient's regular care, should not be disclosed outside the medical team without the patient's consent. The fact that the third-party doctrine was not even mentioned, not even to reject it, further suggests that it is not relevant here. It might not protect the state hospital from violating the

---

270 *See supra* text accompanying notes 155–58; *see also* Reedy v. Evanson, 615 F.3d 197 (3d Cir. 2010) (finding police request that hospital test patient's blood for drugs, when patient had been tested only for rape treatment, violated Fourth Amendment).

271 *Ferguson*, 532 U.S. at 85 n.24 ("But, as we have noted elsewhere, given the posture of the case, we must assume for purposes of decision that the patients did not consent to the searches, and we leave the question of consent for the Court of Appeals to determine.").

272 Ferguson v. City of Charleston, 308 F.3d 380, 395 (4th Cir. 2002).

273 *Ferguson*, 532 U.S. at 78 (emphasis added) (citations omitted). An important fact in the prior drug testing cases was that no test results were allowed to be turned over to law enforcement authorities; they were used solely by the employer or school to determine eligibility for continued employment or team membership. *Id.* at 79.

Fourth Amendment by voluntarily reporting the test results to government officials.

To be sure, the Court seemed to suggest that some uses of drug test results "involve[] a less serious intrusion on privacy."[274] It noted that a search without individualized suspicion may be reasonable when it serves an important government interest unrelated to law enforcement and the individual's privacy interest is minimal. However, the uses it referenced were confined to the supervisory entity—the employers and schools—who ordered the tests in the first place.[275] It does not specifically address what special needs might justify sending test results to a government agency unrelated to law enforcement, such as a health or social services department.

A third possible conclusion that can be drawn from *Ferguson* is that patients do have a reasonable expectation of privacy in their diagnostic test results. The Court was willing to accord more weight to a patient's medical privacy interests than to other individual interests in privacy, at least those of employees and students. The Court characterized the invasion of privacy in *Ferguson* as "far more substantial" than in its other drug testing cases.[276] Thus, it may be that the government must demonstrate more than a legitimate state interest to qualify for a special needs exception for medical information. The decision rests heavily on the absence of what the Court in *Chandler* calls "any indication of a concrete danger demanding departure from the Fourth Amendment's main rule" requiring individualized suspicion.[277] This suggests that the government's "special need" must be to

---

274 *Id.* at 78.

275 *Bd. of Educ. of Indep. Sch. Dist. No. 92 of Pottawatomie Cnty. v. Earls*, 536 U.S. 822 (2002), *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646 (1995), *Nat'l Treasury Emps. Union v. Von Raab*, 489 U.S 656 (1989), and *Skinner v. Ry. Labor Execs.' Ass'n*, 489 U.S. 602 (1989) all mention a diminished expectation of privacy on the part of those tested, as a result of employment in a safety sensitive government position or attendance at a public school where school officials have responsibility for the students' safety. The Court also considered the procedural reasonableness of the testing policy, including whether the urine sample could be produced behind closed doors, the reliability of the testing laboratory, and the opportunity to check the test results with an independent second opinion.

276 *Ferguson*, 532 U.S. at 78.

277 Chandler v. Miller, 520 U.S. 305, 319 (1997). One might argue that candidates for political office would have a diminished expectation of privacy, yet the Court did not even mention that factor. Instead, taking a cue from Justice Scalia's dissent in *Von Raab*, the Court concluded (with only Chief Justice Rehnquist dissenting) that the testing primarily served a symbolic purpose, to assure the electorate that candidates for office would be free of the influence of drugs. *Id.* at 321–22. Such a purpose was clearly insufficient: "However well meant, the candidate drug test Georgia has devised diminishes personal privacy for a symbol's sake. The Fourth Amendment shields society against that state action." *Id.* at 322.

prevent an identifiable, probably physical, harm, such as a train wreck or an injury to students, that could plausibly occur if someone under the influence of drugs were not excluded from participation.[278] The *Chandler* Court concluded:

> [W]here the risk to public safety is substantial and real, blanket suspicionless searches calibrated to the risk may rank as 'reasonable'—for example, searches now routine at airports and at entrances to courts and other official buildings. But where, as in this case, public safety is not genuinely in jeopardy, the Fourth Amendment precludes the suspicionless search, no matter how conveniently arranged.[279]

If the special needs exception were limited to circumstances in which individuals pose a threat to public safety, then many reporting requirements could be challenged.[280] Together, *Ferguson* and *Chandler* suggest that the ultimate—and vague—goal of improving public health in general would not qualify as a special need that justifies a suspicionless search.

Two recent lower court cases support this conclusion. The Eleventh Circuit found that a Florida statute requiring suspicionless drug testing of all applicants as a condition of eligibility for Temporary Assistance for Needy Families ("TANF") benefits violated the Fourth Amendment.[281] The court concluded that the state failed to establish a special need to test all applicants without any suspicion.[282] The state

---

278 The *Chandler* decision emphasized that the testing requirement was "not needed and cannot work to ferret out lawbreakers," because that goal could be accomplished with ordinary law enforcement methods, including warrants. *Id.* at 320. However, the Court was far more deferential to the schools in *Vernonia* and *Earls*, despite the lack of evidence of danger from drug use among students. In *Earls*, the Court emphasized the school's "custodial and tutelary responsibility for children" as the primary legitimate basis for testing. 536 U.S. at 830. Such differences suggest an approach to drug testing that depends upon the Court's view of the population targeted for testing. *See generally* George M. Dery, III, *Are Politicians More Deserving of Privacy Than Schoolchildren? How* Chandler v. Miller *Exposed the Absurdities of Fourth Amendment 'Special Needs' Balancing*, 40 ARIZ. L. REV. 73 (1998).

279 *Chandler*, 520 U.S. at 323 (citation omitted). In *Von Raab*, however, the Court stated that administrative searches are intended "to *prevent* the development of hazardous conditions." 489 U.S at 668. Arguably, students who used drugs could pose some danger to their teammates and teachers during the academic year.

280 One might even consider that the Justices would be sensitive to the fact that their own medical records would be reported under many reporting laws and scrutinize the need for the information as carefully as they did in *Chandler*.

281 Lebron v. Sec'y of Fla. Dep't of Children and Families, 772 F.3d 1352 (11th Cir. 2014).

282 *Id.* at 1364; *see also* Marchwinski v. Howard, 113 F. Supp. 2d 1134, 1144 (E.D. Mich. 2000), *aff'd*, 2003 U.S. App. LEXIS 6893 (6th Cir. 2003) (affirming by an equally divided en banc panel a district court decision enjoining a Michigan statute that authorized the suspicionless drug testing of welfare recipients). The state then settled the case by agreeing to test only recipients who were reasonably suspected of using drugs. Press Release, ACLU, *Settlement Reached in ACLU Lawsuit Over Mandatory Drug Testing of Welfare Recipients*

claimed that drug testing was needed to ensure that (1) beneficiaries meet job readiness goals, (2) TANF meets child-welfare and family-stability goals, and (3) public funds are not used to undermine public health.[283] The court disagreed. It found that, while these were "unquestionably legitimate" public concerns, "these needs are not specific to or special for TANF applicants, nor is drug testing essential to ensuring the success of the TANF program as a whole."[284] Moreover, they are "general concerns, proffered only at a high level of abstraction and without empirical evidence, and thus do not justify an exception to the Fourth Amendment."[285]

The court required a "substantial" special need—a purpose "important enough to override the individual's acknowledged privacy interest, sufficiently vital to suppress the Fourth Amendment's normal requirement of individualized suspicion."[286] Moreover, the state had the burden of demonstrating a special need before the court needed to balance that need against the privacy interest at stake.[287]

The Eleventh Circuit also rejected Florida's alternative claim that applicants consented to the tests. Specifically, the court confirmed that the state cannot conduct unconstitutional drug tests "indirectly by conditioning the receipt of this government benefit on the applicant's forced waiver of his Fourth Amendment right."[288] The fact that the test was required as a condition of TANF benefits rendered it involuntary and, therefore, not a valid consent. Such a required "consent" does not render a search reasonable for purposes of the Fourth Amendment.[289] Perhaps more importantly, the court made clear its view that consent is not an independent justification for a special needs search. Rather, when a government benefit is conditioned on

---

(Dec. 18, 2003), http://www.aclu.org/news/settlement-reached-aclu-michigan-lawsuit-over-mandatory-drug-testing-welfare-recipients.

283 *Lebron*, 772 F.3d at 1359, 1364; *see generally* Brianna W. McLaughlin, *Drug Testing, Welfare, and the Special Needs Doctrine: An Argument in Support of Drug Testing TANF Recipients*, 61 CLEV. ST. L. REV. 567 (2013) (arguing for suspicionless testing of all TANF applicants to protect children and save the state money).

284 *Lebron*, 772 F.3d at 1364.

285 *Id.* The court found that the state's interests apply generally to everyone in the state, not only TANF applicants, but then noted that "the State does not—and cannot—claim an entitlement to drug test all parents of all children." *Id.*

286 *Id.* at 1364 (quoting Chandler v. Miller, 520 U.S. 305, 318 (1997)).

287 *Id.*; *see also* New Jersey v. T.L.O., 469 U.S. 325, 351 (1985).

288 *Lebron*, 772 F.3d at 1374; *accord* Am. Fed'n of State, Cnty. & Mun. Emps. Council 79 v. Scott, 717 F.3d 851, 873 (11th Cir. 2013) ("In effect, the State is offering its employees this Hobson's choice: either they relinquish their Fourth Amendment rights and produce a urine sample which carries the potential for termination, or they accept termination immediately.").

289 *Lebron*, 772 F.3d at 1375; *Scott*, 717 F.3d at 875.

consent to drug testing, "the unconstitutional conditions inquiry is baked into the special needs analysis."[290] Instead, the degree of voluntariness of any consent goes to the level of the person's expectation of privacy in the special needs analysis.

Of course, these special needs cases all concern requiring a person to take a drug test, whereas reporting laws simply require third parties to turn over the person's test results or other medical information to government. A district court decision that may offer some insight into mandatory reporting laws is *Oregon Prescription Drug Monitoring Program v. U.S. Drug Enforcement Administration*.[291] Oregon created a PDMP to help physicians and pharmacists identify drugs their patients use for purposes of recognizing drug interactions and drug-seeking behavior.[292] The state statute barred disclosures to federal, state, and local law enforcement agencies unless they were made "[p]ursuant to a valid court order based on probable cause" in an authorized drug-related investigation involving a person whose information is requested.[293] The state sought declaratory judgment that the Oregon statute precluded the federal Drug Enforcement Administration ("DEA") from demanding PDMP data without a court order. The DEA had repeatedly served the PDMP with administrative subpoenas seeking data about individuals, asserting that the Controlled Substances Act authorizes it to obtain such information by subpoena alone and preempts the Oregon law.[294] Importantly, the DEA relied on the third-party doctrine to argue that patients have no reasonable expectation of privacy in their information submitted to the PDMP.[295]

The district court held that the patients whose data was in the PDMP and physicians who used the PDMP for medical purposes had a reasonable expectation of privacy in their prescription information.[296] Given this "heightened privacy interest," the court found that demanding the data by issuing administrative subpoenas would be an unreasonable search in violation of the Fourth Amendment.[297] The third-party doctrine did not apply here, said the court, because "patients and doctors are not voluntarily conveying information to the PDMP," and the PDMP records are "more inherently personal or

290 *Lebron*, 772 F. 3d at 1376.

291 998 F. Supp. 2d 957 (D. Or. 2014).

292 *Id.* at 959–60 (noting that the PDMP recorded prescriptions for Schedules II-IV drugs under the federal Controlled Substances Act).

293 *Id.* at 960 (quoting Or. Rev. Stat. § 431.964, § 431.966).

294 *Id.* at 961; *see also* 21 U.S.C. § 876.

295 *Or. Prescription Drug Program*, 998 F. Supp. 2d at 966.

296 *Id.* at 964, 966.

297 *Id.* at 967.

private" than the business records at issue in *Miller* and *Smith v. Maryland*.[298] Accordingly, the DEA would be required to obtain a court order to obtain specific PDMP records.

VI. THE FIFTH AND FOURTEENTH AMENDMENTS

We turn now to conceptions of reasonable expectations of privacy in personal medical information that might warrant due process protection under the Fifth and Fourteenth Amendments. State mandatory reporting laws have rarely received judicial review. The few United States Supreme Court decisions touching the subject have granted substantial, but not unlimited, deference to state legislatures to compel reporting of prescriptions for controlled substances (with patient names) to deter and investigate drug crimes, and to report cases of abortion (without patient names) for maternal health research and statistical summaries.

Whalen v. Roe, decided in 1977, might be considered a foundational case in this area.[299] *Whalen* has been cited for the proposition that the state can collect identifiable medical information for legitimate purposes, using something akin to minimum scrutiny.[300] It has also been cited as recognizing or at least indicating that a person has a constitutionally protected expectation of privacy in his or her medical information.[301] Neither of these propositions completely captures the nuances in *Whalen*'s facts or opinion. Like *Miller*, *Whalen* offers less guidance for contemporary data collection and use than might be assumed.

Whalen upheld a New York state law requiring pharmacies to send a copy of every prescription for Schedule II drugs to the state health

298 *Id.* (citing United States v. Golden Valley Elec. Ass'n, 689 F.3d 1108, 1116 (9th Cir. 2012)). *But see* State v. Wiedeman, 835 N.W.2d 698 (Neb. 2013) (upholding law enforcement search of a patient's prescription records at pharmacies because patient had no ownership or possessory interest in records); Williams v. Kentucky, 213 S.W.3d 671, 683–84 (Ky. 2006) (upholding Kentucky All-Schedule Prescription Electronic Reporting program as facially constitutional).

299 Whalen v. Roe, 429 U.S. 589 (1977).

300 *See e.g.*, Act-Up Triangle v. Com'n for Health Serv., 483 S.E.2d 388, 395 (N.C. 1997) (upholding an AIDS reporting law that enforced the confidentiality of medical records with criminal and civil penalties); Stone v. Stow, 64 Ohio St. 3d 156, 166, 593 N.E.2d 294, 301 (Ohio 1992) (citing *Whalen* for proposition that privacy in prescription records is limited to prohibiting disclosure to the public).

301 *See, e.g.*, Nat'l Aeronautics & Space Admin. v. Nelson, 131 S. Ct. 746, 756–57 (2011); Big Ridge, Inc. v. Fed. Mine Safety and Health Review Comm., 715 F.3d 631, 648 (7th Cir. 2013); Coffman v. Indianapolis Fire Dep't, 578 F.3d 559, 566 (7th Cir. 2009); United States v. Westinghouse Elec. Corp., 638 F.2d 570, 577 (3d Cir. 1980).

department.[302] The prescriptions, which included the patient's name, address, and age, were used to identify unlawful drug prescribing and dispensing and unlawful drug diversion.[303] Patients and physicians challenged the statute, claiming a right to privacy grounded in both the Fourth and Fifth Amendments (through the Fourteenth Amendment).[304]

The Court did not discuss the Fourth Amendment, relegating the issue to a footnote. There it rejected the challengers' reliance on *Katz v. United States*[305] and *Terry v. Ohio*,[306] saying, "those cases involve affirmative, unannounced, narrowly focused intrusions into individual privacy during the course of criminal investigations. We have never carried the Fourth Amendment's interest in Privacy as far as the [Whalen] appellees would have us. We decline to do so now."[307] The Court's decision in *Miller*, decided the year before, must have been fresh in the Justice's minds. Still, the Court's footnote is puzzling, since the prescription data were intended to be used to discover and initiate investigations of drug-related criminal offenses, as well as violations of medical or pharmacy licensure. In this respect, they were somewhat similar to administrative searches to which the Fourth Amendment does apply. Perhaps the real distinction lay in the fact that the prescriptions were collected as an ongoing program, rather than a single, "narrowly focused intrusion."

The challengers objected to (1) the state's initial collection of their identifying information, as well as (2) the possibility that their information would be exposed to others. The Court recognized both claims, but focused on the latter. It framed the claim under the Fourteenth Amendment, primarily as "the individual interest in avoiding disclosure of personal matters," which it distinguished from the "interest in independence in making certain kinds of important decisions."[308]

---

302 Controlled Substances Act, 21 U.S.C. §§ 801 et seq.

303 *Whalen*, 429 U.S. at 593. The state sought to prevent patients from stealing prescriptions or obtaining drugs from multiple physicians, pharmacists from improperly refilling prescriptions, and physicians from overprescribing. *Id.* at 592.

304 *Id.* at 598.

305 389 U.S. 347 (1967).

306 392 U.S. 1 (1968).

307 *Whalen*, 429 U.S. at 604 n.32.

308 *Id.* at 599–600. The latter reference was to the right to privacy that includes the right to make decisions about marriage, contraception and abortion. Loving v. Virginia, 388 U.S. 1 (1969); Griswold v. Connecticut, 381 U.S. 497 (1965). The Court had decided *Roe v. Wade*, 410 U.S. 113 (1973) only four years earlier. With the contours of this right to privacy still being developed, the Court had little precedent to rely on. Later, in the abortion reporting cases, the Court seemed to find both aspects of privacy at issue, since man-

The Court's reasons for finding no Fourteenth Amendment violation in *Whalen* may not tell us much about the validity of modern mandatory reporting laws. First, the Court found that the state protected the confidentiality of the data by keeping them on magnetic tapes in an offline computer in a locked room and limiting the number of people authorized to access the data.[309] That is not a realistic option today. Computing has changed dramatically since 1977. Mandatory reports are increasingly sent to health departments electronically through a secure internet portal. Still, breaches remain a worry.[310] In addition, today's data are made available to multiple third parties for various uses.[311] Indeed, that is the purpose of creating many databases.

Second, the Court analogized the prescription law to laws requiring the reporting of venereal disease, child abuse, and deadly weapon wounds.[312] The first example enables an early response to an immediate threat to other people. The latter two are related to investigating possible criminal offenses. The number of reporting laws has increased significantly since 1977. Most of these collect data not for such immediate uses, but for future analysis and research. It is unlikely that the Court considered the extent to which future laws would sweep up data for far less immediate purposes.

Third, the prescription reporting law in *Whalen* can be viewed as adding a mechanism for enforcing the state's criminal laws against unlawful prescribing and unlawful drug use, even if the forms were

---

datory reporting of abortion information could chill the exercise of the right to decide to have an abortion. Perhaps for that reason, the Court approved reporting laws that did not include the patient's name. *See* Planned Parenthood of Se. Pa. v. Casey, 505 U.S. 833, 900–01 (1992); Thornburgh v. Am. Coll. of Obstetricians and Gynecologists, 476 U.S. 747, 765–68 (1986); Bellotti v. Baird, 443 U.S. 622 (1979); Planned Parenthood of Cent. Mo. v. Danforth, 428 U.S. 52, 80–81 (1976).

309 *See Whalen*, 429 U.S. at 605–07 (Brennan, J., concurring) ("The central storage and easy accessibility of computerized data vastly increase the potential for abuse of that information, and I am not prepared to say that future developments will not demonstrate the necessity of some curb on such technology.").

310 *See, e.g.*, Robert Hackett, *Massive Federal Data Breach Affects 7% of Americans*, TIME.COM (July 9, 2015), http://time.com/3952071/opm-data-breach-federal-employees/; U.S. Dep't of Health and Human Servs. *Data breach results in $4.8 million HIPAA settlements*, HHS Press Office (May 7, 2014), http://www.hhs.gov/news/press/2014pres/05/20140507b.html; U.S. Dep't of Health and Human Servs., *WellPoint Pays HHS $1.7 Million for Leaving Information Accessible over Internet*, HHS Press Office (July 11, 2013), http:/ /www.hhs.gov/news/press/2013pres/07/20130711b.html; *see also* U.S. Dep't of Health and Human Services, *Office for Civil Rights, Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

311 *See supra* Part II.

312 *Whalen*, 429 U.S. at 602 n.29.

sent to the health department.[313] If so, this would suggest that the Fourteenth Amendment permits collecting data without individualized suspicion for the purpose of future criminal investigations. The special needs line of cases under the Fourth Amendment, however, rejects suspicionless searches for law enforcement purposes.[314] The *Whalen* Court dismissed the application of the Fourth Amendment,[315] but was writing decades before it decided the special needs, drug testing cases like *Ferguson* and *Earls*.

One distinction between these seemingly inconsistent decisions is that the prescriptions in *Whalen* could be used for a few civil purposes, such as medical licensure disciplinary actions, as well as criminal investigations. However, the New York law was enacted in response to a perceived increase in drug crime[316] and was intended to prevent criminal offenses. Thus, another possibility is that the Court was reluctant to strike down a new initiative to attack the drug problem. But the later drug testing programs in *Ferguson*, *Chandler*, *Vernonia* and other cases were also new initiatives to prevent drug use. About the only real distinction is that the drug testing cases involved an immediate response from the entity conducting the tests, whereas the New York law compiled a database for future use. That is not much of a difference. It may simply be that the Court was just beginning to consider whether the Constitution offered any protection from government compelled data collection and was wary of opening the door to a broad principle of privacy.

The Supreme Court has had few opportunities to explain its reasoning. Only a handful of cases concerning health data collection reached the Court after *Whalen*. All those involved laws requiring physicians or hospitals to report medical information about abortions to the health department.[317] These cases, too, offer little guidance for analyzing modern reporting laws. First, the reporting requirement was a relatively minor issue in cases that challenged restrictions on a

---

313 *Id.* at 603 n.30 (noting that it is "well settled that the State has broad police powers in regulating the administration of drugs by the health professions"); *see also* State v. Russo, 790 A.2d 1132, 1157 (Conn. 2002) *cert denied* 537 U.S. 879 (2002) (describing *Whalen* as not distinguishing between law enforcement and health department access to prescription records and recognizing that the New York law was passed "to prevent *criminal* misconduct" (emphasis in original)).

314 *See supra* Part V.

315 *See supra* text accompanying note 307.

316 *Whalen*, 429 U.S. at 591–92.

317 *See, e.g.*, Planned Parenthood of Se. Pa. v. Casey, 505 U.S. 833, 900–01 (1992); Thornburgh v. Am. Coll. of Obstetricians and Gynecologists, 476 U.S. 747, 765–68 (1986); Bellotti v. Baird, 443 U.S. 622 (1979); Planned Parenthood of Cent. Mo. v. Danforth, 428 U.S. 52, 80-81 (1976).

woman's right to decide whether to terminate a pregnancy and, accordingly, received little analysis. Second, while the Court recognized a right to privacy, it did not always distinguish between information privacy and the liberty interest in making decisions about abortion.

In *Danforth*, the Court upheld a Missouri statute requiring abortion data reporting for the purpose of preserving "maternal health and life by adding to the sum of medical knowledge through the compilation of relevant maternal and health and life data and to monitor all abortions performed to assure that they are done only under and in accordance with the provisions of the law."[318] It concluded, "Recordkeeping and reporting requirements that are reasonably directed to the preservation of maternal health and that properly respect a patient's confidentiality and privacy are permissible."[319] What counts as proper respect for privacy was not explained. The statute did not expressly require the patients' names or other identifying information, and it limited use to "statistical purposes." The Court noted that the requirements were "perhaps approaching impermissible limits," but were "not constitutionally offensive in themselves," as long as they were not "abused or overdone."[320]

In contrast, the Court struck down a Pennsylvania statute that did exceed permissible limits. The law required detailed information about abortion patients, including age, race, marital status, political subdivision, payment method, number of prior pregnancies and gestational age, and also allowed abortion records to be "open to public inspection and copying."[321] The Court found that three of the law's characteristics "belie[d] any assertions . . . that [the state] is advancing any legitimate interest."[322] These were the "scope of information required," despite the fact that names were not required, "its availability to the public," and the lack of limitations on how the information could be used.[323]

In *Planned Parenthood of Southeastern Pennsylvania v. Casey*, however, the plurality opinion seemed to favor data collection for the purpose

318 *Danforth*, 428 U.S. at 81.

319 *Id.* at 80.

320 *Id.* at 81.

321 *Thornburgh*, 476 U.S. at 765–68.

322 *Id.* at 765.

323 *Id.*; *see also id.* at 766–67 ("Although the statute does not specifically require the reporting of the woman's name, the amount of information about her and the circumstances under which she had an abortion are so detailed that identification is likely. . . . The 'impermissible limits' that *Danforth* mentioned and that Missouri approached have been exceeded here.").

of medical research: "The collection of information with respect to actual patients is a vital element of medical research."[324] The statute required reporting the physician, the facility, the referring physician or agency, the woman's age (but not her name), the number of prior pregnancies and abortions, gestational age, type of abortion procedure, date of abortion, any preexisting medical conditions that could complicate abortion, the basis for deciding whether the abortion was medically necessary, if relevant, weight of the aborted fetus, and whether the woman was married. In the Court's view, the data to be reported did not pose a substantial obstacle to a woman's choice.[325]

The Court's focus in the abortion decisions appears to be whether the disclosure of information would chill the exercise of a constitutional right by "requiring disclosure of protected, but sometimes unpopular, activities."[326] Thus, the Court paid close attention to whether a woman could be identified from the reported information.

Lower courts, however, have recognized a more specific constitutional right to privacy in one's personal medical information.[327] In *Tucson Woman's Clinic v. Eden*, for example, the Ninth Circuit Court of Appeals specifically addressed information privacy separately from the right to decide to have an abortion and also from a Fourth Amendment claim.[328] It struck down state law provisions requiring abortion providers to allow health department personnel access to patient medical records (including names and addresses) and to give fetal ultrasound prints to private contractors as violations of the patients' right to information privacy.[329] Earlier, the Ninth Circuit had held that the right to informational privacy "applies both when an individual chooses not to disclose highly sensitive information to the government and when an individual seeks assurance that such information will not be made public."[330] In *Tucson Woman's Clinic*, the court said, "Even if a law adequately protects against *public* disclosure of a patient's private information, it may still violate informational

---

324 Planned Parenthood of Se. Pa. v. Casey, 505 U.S. 833, 900–01 (1992).

325 The Court nevertheless struck down the requirement to report the woman's reason for not notifying her husband as an undue burden, because its opinion also invalidated the statute's provision compelling married women to notify their husbands as an undue burden on a woman's right to choose. *Id.* at 901.

326 *Thornburgh*, 476 U.S. at 747; *see also* MARINER & ANNAS, *supra* note 33, at 438.

327 State constitutions also protect privacy, often more explicitly than the federal constitution. *See, e.g.*, Hill v. Nat'l Collegiate Athletic Ass'n, 865 P.2d 633, 641 (Cal. 1994) (medical records).

328 Tucson Woman's Clinic v. Eden, 371 F.3d 1173, 1180 (9th Cir. 2004).

329 *Id.*

330 Planned Parenthood v. Lawall (*Lawal II*), 307 F.3d 783, 798–90 (9th Cir. 2002).

privacy rights if an unbounded, large number of government employees have access to the information."[331] The court found that the state had little, if any, need for much of the information sought; most of the information bore no relation to patient health or safety.

Outside the context of mandatory reporting laws, federal courts of appeal have recognized Fourteenth Amendment protection for a person's privacy interest in personal medical information and from involuntary disclosure to state and federal agencies.[332] Many of these

331 *Tucson Woman's Clinic*, 371 F.3d at 1193 (emphasis in original).

332 *See* Moore v. Prevo, 379 F. App'x 425, 428 (6th Cir. 2010) (holding that prisoners have a "Fourteenth Amendment privacy interest in guarding against disclosure of sensitive medical information from other inmates"); O'Connor v. Pierson, 426 F.3d 187, 201 (2d Cir. 2005) (psychiatric records); Doe v. Delie, 257 F.3d 309, 315 (3d Cir. 2001) (inmate's HIV status); Livsey v. Salt Lake Cnty., 275 F.3d 952, 956 (10th Cir. 2001) (stating that if information is "highly personal or intimate," like sexual medical information, an individual's expectation of privacy is legitimate); Sterling v. Borough of Minersville, 232 F.3d 190 (3d Cir. 2000) (sexual orientation); Gruenke v. Seip, 225 F.3d 290, 302–03 (3d Cir. 2000) (minor student's pregnancy status); Denuis v. Dunlap, 209 F.3d 944, 956 (7th Cir. 2000) ("[T]he right clearly covers medical records and communications."); Herring v. Keenan, 218 F.3d 1171, 1175 (10th Cir. 2000), *cert. denied*, 122 S. Ct. 96 (2001) (medical information); Bartnicki v. Vopper, 200 F.3d 109, 122 (3d Cir. 1999) ("The right not to have intimate facts concerning one's life disclosed without one's consent" is "a venerable [right] whose constitutional significance we have recognized in the past.") (citing Paul P. v. Verniero, 170 F.3d 396, 401–02 (3d Cir. 1999)); Powell v. Schriver, 175 F.3d 107, 111 (2d Cir. 1999) (transexualism); Doe v. Se. Pa. Trans. Auth. (SEPTA), 72 F.3d 1133, 1137 (3d Cir. 1995) (public employee's "medical prescription record is . . . protected by the Constitution"); Anderson v. Romero, 72 F. 3d 518, 522 (7th Cir. 1995); Doe v. City of New York, 15 F.3d 264, 267 (2d Cir. 1994) ("Individuals who are infected with the HIV virus clearly possess a constitutional right to privacy regarding their condition."); Lankford v. City of Hobart, 27 F.3d 477, 479 (10th Cir. 1994) (finding that "an employee's medical records, which may contain intimate facts of a personal nature, are well within the ambit of materials entitled to privacy protection" (citations omitted)); A.L.A. v. West Valley City, 26 F.3d 989, 990 (10th Cir. 1994) ("There is no dispute that confidential medical information is entitled to constitutional privacy protection."); Alexander v. Peffer, 993 F.2d 1348, 1351 (8th Cir. 1993) (concerning "highly personal medical and financial information"); Watson v. Lowcountry Red Cross, 974 F.2d 482 (4th Cir. 1992); Walls v. City of Petersburg, 895 F.2d 188, 194 (4th Cir. 1990); Schaill v. Tippecanoe Cnty. Sch. Corp., 864 F.2d 1309, 1322 n.19 (7th Cir. 1989) (finding "a substantial privacy interest in the confidentiality of medical information"); Fraternal Order of Police v. City of Philadelphia, 812 F.2d 105, 112–13 (3d Cir. 1987) ("The more intimate or personal the information, the more justified is the expectation that it will not be subject to public scrutiny." involving a police investigator's medical, financial and behavioral information); In re Search Warrant (Sealed), 810 F.2d 67, 71 (3d Cir. 1986), *cert. denied*, 483 U.S. 1007 (1987) (medical records); Trade Waste Mgmt. Ass'n, Inc. v. Hughey, 780 F.2d 221, 234 (3d Cir. 1985) (personal medical history protected from random government intrusion); Taylor v. Best, 746 F.2d 220, 225 (4th Cir. 1984), *cert. denied*, 474 U.S. 982 (1985); United States v. Westinghouse Elec. Corp., 638 F.2d 570 (3d Cir. 1980) (holding that NIOSH could compel production of employee medical records from private corporation for investigation of employee complaints and listing criteria for disclosure); Schachter v. Whalen, 581 F.2d 35, 37 (2d Cir. 1978) (finding a constitutionally protected "interest in avoiding disclosure of

have required heightened scrutiny of laws that provide access to health or sexual information.[333] However, the cases do not necessarily offer a coherent, overall conception of expectations of health information privacy. Rather, many appear to consider the sensitivity of specific information requests on a case-by-case basis.[334] Mark Rothstein has argued that a few courts appear to be narrowing constitutional due process protection for medical information privacy.[335] In *Matson v. Board of Education*, for example, a majority of judges found no constitutional protection without a showing of "societal discrimination and intolerance against those suffering from" a particular disease—fibromyalgia.[336] This places a substantial burden on individuals, whose primary injury is often the dignitary harm of disclosure itself.

VII. TOWARD A MORE NUANCED VIEW OF REPORTING LAWS

The foregoing suggests that while most health-reporting laws subjected to constitutional challenge have been upheld, the cases addressing constitutional questions are limited both in number and relevance. These quasi-precedents do not fit all of today's diverse reporting laws. Data are sought for many different purposes—some essential, others perhaps not. Constitutional doctrines should take

---

personal matters"); Woods v. White, 689 F. Supp. 874, 876 (W.D. Wis. 1988) (prison inmate had a constitutionally protected privacy interest in his medical records and positive HIV test, implicating sensitive information about sexual activity and drug use). *But see* Cutshall v. Sundquist, 193 F.3d 466, 481 (6th Cir. 1999) (refusing to extend Whalen v. Roe beyond its facts in the absence of specific language in the Constitution defining the right); Doe v. Wigginton, 21 F.3d 733, 740 (6th Cir. 1994) (same); American Fed'n of Gov't Emps., AFL-CIO v. Dep't of Hous. & Urban Dev., 118 F.3d 786, 791 (D.C. Cir. 1997) (doubting a constitutional right of information privacy); J.P. v. DeSanti, 653 F.2d 1080, 1090 (6th Cir. 1981) (same).

333 *See* Sheets v. Salt Lake City, 45 F.3d 1383, 1387 (10th Cir. 1995) (requiring a compelling state interest require disclosure of sexual or health information); Walls v. Petersburg, 895 F.2d 188, 192 (4th Cir. 1990) ("The more intimate or personal the information, the more justified is the expectation that it will not be subject to public scrutiny."); Fraternal Order of Police v. City of Philadelphia, 812 F.2d 105, 110 (3d Cir. 1987) (noting that most circuits apply an "intermediate standard of review" for most confidentiality violations and strict scrutiny for "severe intrusions on confidentiality").

334 For example, courts have allowed disclosure of prison inmates' HIV status to prison guards to protect the prison population in the context of diminished expectations of privacy in the institution. *See, e.g.*, *Anderson*, 72 F.3d at 523; Harris v. Thigpen, 941 F.2d 1495, 1501 (11th Cir. 1991).

335 Mark A. Rothstein, *Constitutional Right to Informational Privacy in Critical Condition*, 39 J. L. MED. & ETHICS 280, 280–81 (2011).

336 Matson v. Bd. of. Educ., City Sch. Dist. of N.Y., 631 F.3d 57, 67 (2d Cir. 2011) (finding no violation of any constitutional right to privacy as a result of public disclosure of public school teacher's fibromyalgia).

the differences into account when determining the scope of privacy and justifiable government uses of identifiable data for civil purposes.

Interpretations of the human right to privacy do take such differences into account. For this reason, they may offer standards against which to evaluate the merits of diverse reporting laws.[337] First, as the High Commissioner's *Report on Privacy* makes clear, the human right to privacy embodies the core principles of legality, necessity, and proportionality.[338] State interference with an individual's "privacy, family, home or correspondence"[339] must first be lawful, in the sense of duly authorized by legitimate institutions. But, proper authorization does not save a law from being arbitrary and therefore in violation of the Covenant.[340] The Human Rights Committee explains that to avoid arbitrariness, laws must be "in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstance."[341] Thus, just as U.S. laws must not violate constitutional rights, laws in States party to the Convention, including the United States, are bound not to contravene the human rights protected by the Convention.

The concept of necessity refers to the State's justification for obtaining identifiable information: "public authorities should only be able to call for such information relating to an individual's private life the knowledge of which is essential in the interests of society as understood under the Covenant."[342] This suggests a level of justification that exceeds what might count as a legitimate state interest for due process purposes. It is buttressed by the proportionality (or reasonableness) requirement, which implies that "any interference with privacy must be proportional to the end sought and be necessary in the

337 Although limited to criminal laws, the AMERICAN BAR ASSOCIATION STANDARDS FOR CRIMINAL JUSTICE, LAW ENFORCEMENT ACCESS TO THIRD PARTY RECORDS (3d ed. 2013) might also serve as a partial model for government access to records for civil purposes. The Standards categorize information held by institutional third parties as "highly private, moderately private, minimally private, or not private," with the level of protection decreasing protection with the degree of privacy. *Id.* at 19. The Standards also recognize the ubiquity of data disclosure to third parties today. Accordingly, they recommend that legislative authorizations to access data consider, *inter alia*, "the extent to which (a) the initial transfer of such information to an institutional third party is reasonably necessary to participate meaningfully in society or in commerce, or is socially beneficial." *Id.* at 20.

338 OHCHR, Right to Privacy, *supra* note 14, at 49.

339 *Id.* at 55.

340 Human Rights Committee, *supra* note 20, at para. 3.

341 *Id.* at para. 4.

342 *Id.* at para. 7.

circumstances of any given case."[343] These principles recognize that privacy is not a one-dimensional right, but contains components of varying sensitivity and importance. The case-specific focus also calls for tailoring demands for identifiable information to the importance of the government's need.

The Human Rights Committee also requires States to take "[e]ffective measures . . . to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant."[344] This is consistent with an admonition to limit custody and use of the information collected to those with specific authority to do so. It may limit the extent to which identifiable data in a government database can be disclosed to third parties for different uses than that for which it was originally collected.

U.S. cases discussing due process protection of privacy tend to use a balancing test that weighs the purpose of data collection against the intrusion on a person's privacy. While the concept of balancing might fit the human rights framework, both sides of the scale are often stated in frustratingly general terms in U.S. case law.[345] Purposes are often briefly described as broad societal goals like reducing drug abuse[346] or medical research.[347] No one would argue with such noble aspirations. Yet, such goals fail to meaningfully explain the real purpose for which data will be used and why the data are needed.[348] This makes it difficult to assess the weight of the state's interest. The connection between data collection and these general goals is often speculative and far in the future. For example, APCDs hope to use

---

343 Human Rights Committee, 50th Sess., Commc'n No. 488/1992: Australia 04/04/94, CPR/C/50/D/488/1992, at 9 (Mar. 31, 1994), http: //www1.chr.up.ac.za/undp/other/docs/caselaw15.pdf.

344 Human Rights Committee, *supra* note 20, at para. 10.

345 *See* Christopher Slobogin, *The World Without a Fourth Amendment*, 39 UCLA L. REV. 1, 106–07 (1992) (describing how Supreme Court Justices "exaggerate the state's interests [and] trivialize the individual's interests").

346 *See, e.g.*, Whalen v. Roe, 429 U.S. 589, 606 (1977) (Brennan, J., concurring) ("The Court recognizes that an individual's interest in avoiding disclosure of personal matters is an aspect of the right of privacy . . . but holds that in this case, any such interest has not been seriously enough invaded by the State to require a showing that its program was indispensable to the State's effort to control drug abuse." (citations omitted)).

347 *See, e.g.*, Planned Parenthood of Cent. Mo. v. Danforth, 428 U.S. 52, 79 (1976) ("The statute states that the information on the forms 'shall be confidential and shall be used only for statistical purposes.' The 'records, however, may be inspected and health data acquired by local, state, or national public health officers.'")

348 Mariner, *supra* note 73, at 383–84.

insurance claims data to analyze the costs and outcomes of multiple medical services in order to see which are cost-effective. At some future time, after detailed studies, a government agency or private insurer might (or might not) use the study results to alter payment rates. An alteration might (or might not) reduce overall health care costs. At the time of data collection, such results are aspirational and all too often speculative.

Different problems confront the other side of the scale—intrusions on privacy. There may be little consensus on whether the data sought should be considered an aspect of a person's privacy at all. Do people reasonably expect the information to be kept private, and is this expectation socially acceptable? If so, the inquiry proceeds to ask whether requiring disclosure to government would cause the individual measurable harm. In contrast to definitions of purpose, privacy harms are often required to be concrete and imminent.[349] Dignitary harms from being required to reveal identifiable information are rarely considered.[350]

Paradoxically perhaps, several scholars argue that there may be room for a more nuanced standards governing the collection of data from third parties under the Fourth Amendment than under Fifth Amendment due process doctrine.[351] Traditionally, mandatory reporting laws have been slotted into one or more of the exceptions to the Fourth Amendment's requirement of probable cause, warrants, or consent. When closely examined, however, that classification may not hold for some contemporary reporting laws. Furthermore, the possibility that the Supreme Court might begin to apply a mosaic theory[352] to define searches suggests that it may become plausible to bring some civil reporting laws under the Fourth Amendment's protection.

---

349 *See Whalen*, 429 U.S. at 600–04 ("We hold that neither the immediate nor the threatened impact of the patient-identification requirements in the New York State Controlled Substances Act of 1972 on either the reputation or the independence of patients for whom Schedule II drugs are medically indicated is sufficient to constitute an invasion of any right or liberty protected by the Fourteenth Amendment."); *see also* Mariner, *supra* note 73, at 377–81.

350 *But see* Nw. Mem'l Hosp. v. Ashcroft, 362 F.3d 923 (7th Cir. 2004) (considering how women would feel if their abortion records or photos of their torsos were made publicly available even without identification).

351 *See* Henderson, *supra* note 146.

352 *See* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012); *see also* United States v. Jones, 132 S. Ct. 945, 963–64 (Alito, J., concurring); *id.* at 956 (Sotomayor, J., concurring) (determining whether government behavior constitutes a search requires considering "whether people reasonably expect that their movements will be recorded and aggregated" in such a manner).

The Supreme Court has grounded its conceptions of Fourth Amendment privacy in various ways, often using a property or boundary-based theory of privacy, while at other times expressing a reasonable expectations of privacy theory.[353] The property-based theory asks whether police (typically) have crossed over from public to private property, such as a house.[354] The reasonable expectations theory asks whether a person has a reasonable expectation of privacy in something, such as the contents of a telephone call[355] or a suitcase,[356] even when the telephone or suitcase is in a public place.[357] While the *Jones* decision appeared to rely on a property-based theory of trespass,[358] *Riley* was concerned with the expectation of privacy in cell phone content.[359] The variation in rationales in these cases suggests that the Court looks not merely to a single action on the part of government, such as viewing cell phone contents, but also considers the government's reason for seeking the information and the degree to which the information sought deserves constitutional protection.

Changes in Fourth Amendment doctrine would require finding that government demands for information from third parties constitute a search, determining whether the search requires a warrant, and if not, whether it is reasonable without a warrant.[360] The first issue entails express recognition that the third-party doctrine does not apply as a blanket exception. The second and third issues are likely

353 *See, e.g.*, California v. Greenwood, 486 U.S. 35, 39 (1988); Rakas v. Illinois, 439 U.S. 128, 143 (1978).

354 *See, e.g.*, Florida v. Jardines, 133 S. Ct. 1409, 1417 (2013); Kyllo v. United States, 533 U.S. 27 (2001).

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

356 *See, e.g.*, Bond v. U.S., 529 U.S. 334 (2000) (tactile examination of bus passenger's luggage in overhead storage violated the Fourth Amendment). For a deeper analysis of Fourth Amendment protections for luggage see generally Jason W. Eldridge, *The Fourth Amendment: The Privacy of Overhead Luggage Compartments on Commercial Buses*, 27 WM. MITCHELL L. REV. 2003 (2001).

357 *See Katz*, 389 U.S. at 351 (arguing that "the Fourth Amendment protects people not places").

358 *Jones*, 132 S. Ct. at 951 n.5.

359 *See* Riley v. California, 134 S. Ct. 2473, 2484 (2014) ("These cases require us to decide how the search incident to arrest doctrine applies to modern cell phones . . . ."); United States v. Davis, 754 F.3d 1205, 1216 (11th Cir. 2014) (finding a reasonable expectation of privacy in cell phone site location information whose exposure "can convert what would otherwise be a private event into a public one"); *see also* Commonwealth v. Augustine, 4 N.E.3d 846 (Mass. 2014) (finding a reasonable expectation of privacy in cell phone data; third-party doctrine did not apply; warrant required).

360 Maryland v. King, 133 S. Ct. 1958, 1970 (2013) ("Even if a warrant is not required, a search is not beyond Fourth Amendment scrutiny; for it must be reasonable in its scope and manner of execution.").

to be fact specific.[361] They would depend on both the nature of the information sought (to evaluate its privacy quotient) and the reason for seeking it.[362] Such factual variations, however, should not pose insurmountable obstacles for the judiciary when applied to reporting laws. Unlike cases involving criminal investigations of individuals, reporting laws offer a single reason (or state interest) for collecting a particular category of information. Thus, there is no need to address individual variations. Each law can be analyzed in categorical terms.[363]

Even in the absence of formal doctrinal change, some Fourth Amendment cases use reasoning parallel to that used in due process analyses—assessing whether government has a legitimate reason for obtaining personal information that qualifies as private.[364] Thus, courts have already demonstrated their capacity to perform the requisite analysis.

This does raise the question whether the tests for Fourth and Fifth Amendment purposes are or should be considered the same or even duplicative? Is there any meaningful difference between a due process justification and a special need for information? If there are none, then perhaps granting Fourth Amendment protection to health information held by third parties gains nothing for those who seek more privacy protection.

---

361 Kerr argues for retaining a blanket third-party doctrine in order to avoid fact-specific queries that complicate law enforcement decision-making. *See generally* Kerr, *supra* note 102.

362 *See generally* SOLOVE, *supra* note 30 (arguing for variation in privacy protections depending on the type of information, its intended use, and the risk of different harms).

363 One might argue that the categorical nature of civil reporting laws makes data collection reasonable within the meaning of the Fourth Amendment, because uniform reporting requirements limit government discretion and opportunities for abuse, such as targeting disfavored individuals. *See generally* Stephen E. Henderson, *Fourth Amendment Time Machines (and What They Might Say About Police Body Cameras)*, 18 U. PA. J. CONST. L. 933 (2016). The legislature can duly weigh the importance of the government interest against reasonable expectations of privacy. In theory, the powerful and affluent, who are affected along with the disadvantaged, can protect the individual's interest in privacy through the political process, preventing legislative overreach. *See* William J. Stuntz, *Privacy's Problem and the Law of Criminal Procedure*, 93 MICH. L. REV. 1016, 1944–46 (1995). In practice, however, those most able to exert political influence are unlikely to be aware of the scope of modern reporting laws or moved to engage in legislative debate. In the absence of transparency about civil reporting laws, the political process seems a weak substitute for constitutional review.

364 *See, e.g.*, Samson v. California, 547 U.S. 843, 848 (2006) ("Whether a search is reasonable [under the Fourth Amendment] 'is determined by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.'").

The threshold question in both lines of cases is what counts as a reasonable expectation of privacy that society is or should be prepared to accept as reasonable. While this phrasing comes from *Katz*, the same substance is used in due process cases. Fourteenth Amendment cases support the idea that there is a legitimate and reasonable expectation of privacy in medical information that can be protected from unreasonable searches under the Fourth Amendment. There is nothing wrong with having two or more constitutional amendments that apply to a concept of privacy. The First Amendment can apply to issues of privacy without academic or judicial objection that it conflicts with the application of the Fourth Amendment, for example. Therefore, there should be no impediment to recognizing a person's reasonable expectation of privacy in identifiable health information within the meaning of several Amendments.

One possible difference between Fourth Amendment and due process analysis is the characterization of a justifiable government reason for obtaining personal information. Is a legitimate purpose enough or must government offer a more important state interest? Must the need for data to achieve that purpose be merely plausible or based on empirical evidence? Here, there may be differences. Special needs cases like *Ferguson* indicate that the government cannot justify a search for law enforcement purposes, even if the long-term purpose might be a civil benefit to society. Cases like *Whalen* and *Earls* suggest that government can compel information for a legitimate purpose, even if the information is not actually necessary to achieve that purpose.

The question for both Fourth Amendment and due process purposes is whether the government is justified in compelling identifiable health information about individuals. The human rights framework offers principles for refining the doctrine. Specifically, the principles of necessity and proportionality suggest that the state's interest be stated in specific terms, not speculative generalities, and that interest must be "in the interests of society as understood under the Covenant."[365] Moreover, the more sensitive the information at issue, the more justification the state needs to obtain it without consent. Applying the Fourth Amendment would mean that the information warrants protection even in the hands of third parties.

Human rights principles also call for effective remedies for violations.[366] A Fourth Amendment remedy lies in the exclusionary rule,

365 Human Rights Committee, *supra* note 20, at para. 7.

366 *Id.* at para. 11.

which may be sufficient in criminal cases. If the government cannot use the tainted fruit as evidence, a criminal defendant is not harmed, at least in theory. The exclusionary rule has limited practical application in the absence of a criminal prosecution.[367] As in *Chandler*, the often-sought remedy in civil cases is to strike down the law authorizing the search.

Using the human rights framework, it should be possible to categorize reporting laws on the basis of four variables: (1) the sensitivity or expectation of privacy in the health information; (3) the degree of importance of the government function at issue; (4) the magnitude of the need for government to obtain the information to achieve that government function; and (4) the need for individually identifiable data to achieve that government function. As noted above, health information should qualify as sensitive for purposes of the first variable. Most people have a reasonable expectation that their health information will not be used beyond their health care without their consent. Yet that expectation can be overcome for sufficient government purposes.

The second variable focuses on the function that government is performing, rather than a general purpose for collecting the data. This slight shift in terminology from purpose to function is intended to ensure specificity in the statement of a state's interest, which will allow meaningful assessment of its importance. Moreover, it requires all uses of the data to be for a government function. If a government agency expects to provide the data it collects to a third party, that third party must also perform a government function. This would preclude some disclosures to private researchers, but would permit providing relevant data to other government agencies in many cases.

The third variable connects the data to the specific government function by requiring that the data are needed to carry out a government function. This allows government to require the collection of even sensitive data when they are truly necessary to an important purpose of government. The last variable is a reminder that it is identifiable information that raises privacy concerns. To the extent that identifiable data are not necessary, personal identifiers would not be justified.

---

367 *But see* LAFAVE, *supra* note 102, § 1.7(c) (describing how exclusionary rule might apply in civil commitment proceedings); *id.* § 1.7(f) (describing the applicability of exclusionary rule in various administrative proceedings).

Different health reporting laws seek different types of health information for different reasons.[368] Thus, the variables may carry different weights in different laws. See Table 1 below for an example of how reporting laws might be characterized along these parameters.

Using this rubric, mandatory reporting of universal life events that trigger rights and responsibilities of citizenship rank high. These include reports of births, marriages, divorces, and deaths. No one would dispute the government's function in these circumstances or its need to identify an individual with these events. Compelled reporting by hospitals and other agencies should qualify as a civil search that is reasonable under the Fourth Amendment without consent and without probable cause. The rationale is not that the records are produced or held by third parties, but that the government has a legitimate need for identifiable data to carry out an important government function.

Laws requiring the reporting of instances of abuse or neglect of children and vulnerable elderly persons should also rank high, because of the immediacy of the harm and the probability of continued risks to personal safety. Government agencies are properly charged with protecting persons unable to protect themselves, and the identity of wrongdoers is necessary to carry out that function.

Mandatory reporting of contagious diseases and exposure to toxic substances should also rank high. However, more nuance is needed here. It is certainly important for public health officials to identify the source of a dangerous, contagious disease that is spreading in an area or likely to spread very soon. As noted in Part II, instances of disease outbreaks or emerging epidemics are relatively rare, while the list of reportable diseases and conditions is quite long. Today, notifiable diseases must be reported even when the disease poses no immediate threat to anyone but the patient.[369] The reports are used to compile statistics on the incidence and prevalence of diseases and to conduct research on such questions as risk factors for disease. Statistical uses, while important, do not necessarily require identifiable data and may be vulnerable to challenge.

Like notifiable disease reporting laws, contemporary newborn screening laws apply to two categories of conditions. The state has an interest in ensuring that treatable conditions that threaten a newborn's ability to function normally be recognized and brought to the family's attention as soon as possible. However, screening for other

368 *See supra* text accompanying note 85.

369 *See supra* text accompanying notes 71–81.

genetic anomalies only produces samples for DNA databanks that are used for research. Research on how to prevent or treat such conditions is surely important, but it is not an important function for government. As Congress has recognized, such data collection for research requires parental consent.[370]

Reports of cases of chronic conditions are also primarily used for research. They were originally created by hospitals to monitor the quality of care provided by the physicians and others who practiced in that hospital.[371] No one would question that use by caregivers. It is the required collection by government that threatens the legitimacy of such registries. Thus, submission of identifiable data to cancer registries may require individual consent.

It may be justifiable for states to require the creation of registries for uses restricted to non-government entities, such as "information fiduciaries" like health providers. Thus, states might require hospitals to establish cancer registries for the purpose of encouraging hospitals to monitor the quality of care, without requiring any further reporting to the state, as part of the government functions of licensing hospitals and ensuring they provide safe and effective care. Government could also require the establishment of PDMPs with access restricted to physicians and pharmacists, as some are today. But opening such databases to public or private research changes the purpose of collecting the data, removes it from a government function, and undermines its justification. Allowing law enforcement access without a warrant or probable cause comes very close to what *Ferguson* forbids.

The same might be true for immunization registries, which can help both physicians and patients track what immunizations patients have received and when additional doses should be administered. States may have an interest in monitoring whether children have received immunizations required by separate laws that are justified as a means of protecting the public from the spread of contagious diseas-

---

370 *See supra* text accompanying note 79.

371 Cancer registries are the classic example, with a documented history as far back as the late 18th Century. *See* RODOLFO SARACCI & CHRISTOPHER P. WILD, INTERNATIONAL AGENCY FOR RESEARCH ON CANCER: THE FIRST 50 YEARS, 1965–2015, at 106 (2015), http://www.iarc.fr/en/publications/books/iarc50/IARC_50%20years.pdf. Data collection on the incidence and treatment of different cancers was not encouraged by governments until the early 20th Century with Connecticut and New York State leading the way in the United States in the 1940s. *Id.* at 107; *see also State Cancer Registry Laws and Requirements*, AMERICAN ACADEMY OF DERMATOLOGY (Dec. 2012), https://www.aad.org/file%20library/global%20navigation/education%20and%20quality%20care/state%20cancer%20registries/state-cancer-registries-laws-and-requirements.pdf.

es.[372] Since states typically delegate enforcement of immunization laws to schools by making such immunizations a condition for attending school or daycare, it is less clear that other government agencies need or should have access to such registry data without consent.

Many health information registries serve as a repository of data for research. A controversial example is New York City's blood sugar registry.[373] The City's health department argues that individual consent should not be needed because that would "compromise the data analyses that are used to assess the burden of disease, evaluate the impact of interventions, and responsibly allocate government resources."[374] Such arguments logically could apply to a wide range of personal information sought for research.

Some scholars argue that patients should not be allowed to exclude their health information from research databases that are made available to multiple public and private users.[375] The standard arguments for dispensing with consent to research are: (1) the study sample will not be representative of the population as a whole unless everyone is included; and (2) obtaining consent is administratively burdensome and adds costs to the research enterprise.[376] The first argument has always been questionable, if not pretexual. Well-designed research rarely requires information from everyone in a population (either of the country or of those with a particular disease or exposure).[377]

The second argument, although couched in empirical terms, implies a normative claim: it may be difficult for researchers to obtain consent, so the data should be provided without patient consent. Obtaining consent to any type of research (or anything at all) always includes some administrative effort and cost, just as any other aspect of conducting research incurs costs and administrative inconven-

372 *See* Zucht v. King, 260 U.S. 174, 177 (1922) (upholding mandatory immunization against smallpox as a condition of school attendance).

373 *See supra* text accompanying notes 80–81.

374 Chamany et al., *supra* note 82, at 559.

375 *See* Hoffman & Podgurski, *supra* note 1, at 143.

376 *See id.* at 120 (noting that requiring consent would render many research projects cost-prohibitive); IOM RESEARCH, *supra* note 87, at 209–12 (noting that, in some cases, seeking individuals' consent contributes to selection bias); *see also* Lawrence O. Gostin & James G. Hodge, *Personal Privacy and Common Goods: A Framework for Balancing Under the National Health Information Privacy Rule*, 86 MINN. L. REV. 1439, 1451–52 (2002) (arguing that consent would hinder comprehensive data collection and add expense).

377 *See* Mark A. Rothstein & Abigail B. Shoben, *Does Consent Bias Research?*, 13(4) AM. J. BIOETHICS 27, 31–32 (2013).

ience.[378] So the second argument is really a normative claim that autonomy is a lesser value than minimizing cost and inconvenience. If accepted, such a claim would dispense with respect for autonomy and privacy in all circumstances involving money and effort—which means virtually all circumstances.

"Privacy comes at a cost," Chief Justice Roberts said in *Riley*.[379] When government seeks something from an individual, the Constitution requires it to pay the cost, whether by obtaining consent or providing a sufficient justification for not doing so. Convenience is not a sufficient justification. Like privacy, autonomy comes at a cost. Yet no one would claim that cost should always override autonomy. Such a principle would eviscerate such aspects of autonomy as the right to refuse treatment or to participate in research.[380] Absent special circumstances, researchers should not be able to use, for their own research, personally identifiable information collected by a government agency, without the informed consent of the individuals involved, because they would need informed consent in the absence of the database. The database gives them "an effort-free tool" for their research.[381]

The New York City health department made an additional argument to support its blood sugar registry. It said that even if some people do not want to be reported and do not need services, others do, so the possibility that some might benefit should override the objection of the first, perhaps larger, group.[382] This is simply an argument for majority rule, which the Constitution is supposed to constrain. Supporters of the Registry conclude generally that "helping vulnerable people monitor their health status and take measures to reduce risk is well within the government's power."[383] Offering services is certainly within the government's power and should be encouraged. But the reporting ordinance does not offer services; it only compels the reporting of information. If one accepts the idea that a

---

378 *See, e.g.*, Pierce Cnty. v. Guillen, 537 U.S. 129, 146 (2003) (refusing to interpret a federal statute to permit data collected for one purpose to be used for different purposes—as an "effort-free tool"—without complying with any legal prerequisites that would exist in the absence of the database).

379 Riley v. California, 134 S. Ct. 2473, 2493 (2014).

380 Mariner, *supra* note 73, at 394.

381 *Guillen*, 537 U.S. at 146.

382 Chamany et al., *supra* note 82, at 559.

383 Michelle M. Mello & Lawrence O. Gostin, *Commentary: A Legal Perspective on Diabetes Surveillance—Privacy and the Police Power*, 87 THE MILBANK QTRLY. 575, 576 (2009); *see also id.* at 577 (asserting that "the state has a compelling interest in controlling the staggering human, social, and economic burdens of diabetes").

state can obtain personally identifiable health information without the person's consent whenever it might help an agency to offer services, study a disease, plan budgets, or reduce costs, then there really is no limit to the power to compel personal information of any sort.[384]

The most credible arguments for the power to obtain identifiable information for research without consent are still grounded in two empirical requirements, instead of normative principles. The first is an assurance that the study poses no risks of physical or mental harm. Unlike research procedures that interact with the person herself, data collection and analysis do not intrude on the body.[385] To be sure, the revelation of damaging information about a person may cause the person emotional distress or provoke discriminatory actions against the person. Thus, requirements for security and confidentiality are essential: keeping the information secure against revelation outside the research study itself; and ensuring that research results are reported without identifiers and in a manner that prevents attribution to any individual. These are necessary elements of responsible research studies that promise confidentiality. Whether they are sufficient to convince enough people to accept laws authorizing the use of their identifiable information for research is unclear. There may be concern that databases are vulnerable to breach,[386] despite researchers' efforts to provide security, or that information is becoming easier to re-identify.[387] A rigorous survey by Harris Interactive and Alan Westin for the Institute of Medicine found a wide array of public opinions.[388] Only 1% of respondents were willing to allow researchers

384 *See* Mariner, *supra* note 81, at 149–50. The Registry ordinance was not challenged, but it might be vulnerable to challenge. The Board of Health relied on the same law to authorize the Registry as it did to adopt the Portion Cap Rule (a.k.a. Big Gulp). The Portion Cap Rule was struck down on the ground that the Board of Health did not have the legislative authority to issue the ordinance. *See* New York Statewide Coal. of Hispanic Chambers of Commerce v. New York City Dep't of Health & Mental Hygiene, 23 N.Y.3d 681, 701 (N.Y. 2014).

385 *See* IOM RESEARCH, *supra* note 87, at 91–92.

386 *See* Charles Ornstein & Annie Waldman, *CVS Among Hundreds of Providers Violating HIPAA, Review Finds*, THE BOSTON GLOBE (Dec. 29, 2015), https:/ /www.bostonglobe.com/2015/12/29/cvs-veterans-affairs-violate-federal-privacy-laws-review-finds/HPddb5xkuRwiYETmgZKQLN/story.html; Damian Paletta, *Breached Network's Security Is Criticized*, WALL ST. J., June 24, 2015, at A1 (describing problems with federal Office of Personnel Management's security system, which permitted breach).

387 *See Big Data: Seizing Opportunities, Preserving Values*, EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES 54 (May 2014), www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf ("Another reality of big data is that once data is collected, it can be very difficult to keep anonymous.").

388 Alan F. Westin, *How the Public Views Privacy and Health Research*, 20–22 (March 2008), http://www.iom.edu/Object.File/Master/48/528/%20Westin%20IOM%20Srvy%20Rept

to use their personal information without their consent, while 8% were willing to give a general consent to such use.[389] Thirty-eight percent wanted the right to consent to or refuse each use, while 13% would not allow research use under any circumstances.[390]

Most supporters of eliminating consent to health records research assume that such research will bring a new treatment discoveries and significant medical and social benefits. If history offers any lessons, this seems a bit optimistic.[391] Here again, the expected benefits remain speculative and in the future, while erosions of principles of individual autonomy, privacy, and dignity may be immediate. Others may assume that de-identified data will be sufficient for most research.[392] This is also unlikely.[393] Investigators prefer data with personal identifiers for many reasons, including comparing individual results across databases and contacting the individuals for follow-up.[394]

APCDs are a good example of research databases that use individual level data.[395] It would be almost impossible to track health care costs and outcomes without being able to attribute those costs and outcomes to individual patients and physicians. Codes might be sub-

---

%2011-1107.pdf; *see also* Scott Hensley, *Poll: Most Americans Would Share Health Data for Research*, SHOTS—HEALTH NEWS FROM NPR (Jan. 9, 2015, 10:30 AM), http: //www.npr.org/sections/health-shots/2015/01/09/375621393/poll-most-americans-would-share-health-data-for-research (reporting the results of a November 2014 poll showing a decline to 53% [from 68% in an August 2014 poll] of respondents who were in favor of sharing even data that has no identifying information, while 47% would refuse to share even anonymous health data).

389 Westin, *supra* note 388, at 21.

390 *Id.* at 22.

391 *See, e.g.*, Nicolas P. Terry, *Information Technology's Failure to Disrupt Healthcare*, 13 NEV. L.J. 722, 748–49 (2013) (discussing big data's failure to produce significant improvements in health care using Google Health as an example); John P. A. Ioannidis, *Why Most Published Research Findings Are False*, 2 PLOS MED. 696, 699–701 (Aug. 2005), www.plosmedicine.org/article/info:doi/10.1371/journal.pmed.0020124 (finding that initial studies reporting success are typically followed by later studies that fail to replicate the original study's findings, and suggesting reasons for this conclusion).

392 *See, e.g.*, Hoffman & Podgurski, *supra* note 1, at 128.

393 *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymizaton*, 57 UCLA L. REV. 1701, 1716 (2010); Mark A. Rothstein, *Is Deidentification Sufficient to Protect Health Privacy in Research?*, 10 AM. J. BIOETHICS 3, 9 (2010).

394 *See, e.g.*, Frakt & Bagley, *supra* note 46, at 1880 (asserting that the identifiable data in Medicare claims are an "essential variable" for research, and "elaborate consent requirements make it difficult or impossible to share patient data related to substance-use disorders").

395 APCDs also face a claim that ERISA preempts the application of state laws requiring self-insured employee health insurance plans and their third party administrators to submit claims data to the state APCD. *See* Liberty Mut. Ins. Co. v. Donegan, 746 F.3d 497, 508 (2d Cir. 2014) (finding ERISA preempts statute's application to ERISA plans), *cert. granted sub nom.* Gobeille v. Liberty Mut. Ins. Co., 135 S. Ct. 2887 (2015).

stituted for patient names, but many other identifying details are needed to draw meaningful conclusions. Given the pressing need for controlling health care costs, it is certainly important to identify the most cost-effective ways to provide good care. Government agencies at the state and federal level have a legitimate interest in conducting research to do so. But the question of principle intrudes again. The performance of some ordinary government functions includes studies of this sort. How might demands for individually identifiable information for research be distinguished from demands for any other government function? In the absence of a satisfactory distinction, laws requiring third party submission of identifiable data may be vulnerable to challenge.

CONCLUSION

As Justice Marshall wrote, the proper question is what risks people "should be forced to assume in a free and open society."[396] Should people assume the risks associated with government demands for their information, or should the Constitution place limits on those demands? Traditionally, both the Fourth and Fifth Amendments have been interpreted as placing almost all the risk on individuals. However, the Supreme Court's decisions in *Jones*, *Riley*, and *Patel* have inspired hope among scholars who argue that the Fourth Amendment should be a more robust source of information privacy protection. Moreover, international reaction to surveillance is encouraging more attention to enforcing the human right of privacy.[397]

Although this shift in outlook has focused on criminal investigations, it has implications for protecting privacy in the civil sphere. It may inspire challenges to a number of civil laws requiring health providers and insurers to report identifiable health information to the state. While the value of many such laws are beyond question, the rationale for their enactment no longer reflects either the specific purposes they serve in contemporary America or a coherent concept of

396 Smith v. Maryland, 442 U.S. 735, 750 (1979) (Marshall, J., dissenting).

397 *See* OHCHR, Right to Privacy, *supra* note 14, at 4–5 (discussing the right to privacy in the context of governmental digital surveillance in the 2014 report of the Office of the United Nations High Commissioner for Human Rights); Owen Bowcott, *UK-US Surveillance Regime was Unlawful 'For Seven Years'*, THE GUARDIAN (Feb. 6, 2015, 5:10 AM), http://www.theguardian.com/uk-news/2015/feb/06/gchq-mass-internet-surveillance-unlawful-court-nsa (reporting that Great Britain's Investigatory Powers Tribunal found that regulations governing Britain's Government Communications Headquarters' access to phone and email records intercepted by NSA violated Article 8 or 10 of the European Convention on Human Rights).

privacy of medical information. A more nuanced approach to doctrine is in order, one that recognizes the reasonableness of expectations of privacy in health information and demands specific justification for compelling its disclosure to government in accordance with the principles governing the human right of privacy. This approach should distinguish important mandatory reporting laws from fishing expeditions, allow essential data collection, and preserve constitutional protection for essential aspects of privacy.

TABLE 1: REPORTING LAW CHARACTERISTICS

	SENSITIVITY OF HEALTH INFORMATION	IMPORTANCE OF GOVERNMENT FUNCTION	MAGNITUDE OF GOV'T NEED FOR INFORMATION	GOV'T NEED FOR IDENTIFIABLE INFORMATION
Life events (birth, death)	N	H	H	H
Abuse (children, elderly)	M	H	H	H
Serious contagious disease/toxic exposure	H	H	H	H
Treatable newborn genetic condition	H	M	M	H
Controlled substances prescription registry (PDMP)	H	L	M	M
Contagious disease data collection	H	L	M	N
Chronic diseases and conditions	H	L	M	N
Cancer registry	H	L	L	N
Immunization registry	L	M	L	N
Newborn anomalies research	H	N	N	N
Insurance claims research on treatment costs	H	L	M	M
Insurance claims research on treatment quality	H	L	N	M

H = High sensitivity; high importance; high need

M = Moderate sensitivity; moderate importance; moderate need

L = Low sensitivity; low importance; low need

N = NO sensitivity; no importance