NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY

Volume 19
Issue 4 *Online Issue*

Article 11

5-2019

Recent Privacy Law Developments with Major Implications for Medical and Scientific Research

John M. Conley
University of North Carolina School of Law

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
VOLUME 19, ONLINE: MAY 2018

RECENT PRIVACY LAW DEVELOPMENTS WITH MAJOR IMPLICATIONS FOR MEDICAL AND SCIENTIFIC RESEARCH

I. BACKGROUND: HOW PRIVACY LAW AFFECTS MEDICAL AND SCIENTIFIC RESEARCH

Over the last half-dozen or so years, people and companies involved in medical and other scientific research have become increasingly concerned about privacy law, both domestic and international. I base this observation on several things, including the requests for consultation that I receive from lawyers and non-lawyers in the academic and private sectors, the contents of

conferences where I am asked to speak, and my reading of the academic and trade literatures. This concern is entirely rational, as those who do research, whether academic or commercial, are the very kinds of people who need to worry about privacy—of their customers, users, patients, and subjects.

In this essay, I will briefly review three major developments that are having, or likely will have, significant implications for the research community. The first (Part II.A) is international: the European Union's General Data Protection Regulation (GDPR), which takes effect on May 25, 2018. The other two are domestic: the forthcoming revisions to the Common Rule, a regulation that governs all federally funded research in the United Sates (Part II.B); and the Federal Trade Commission's recent foray into the regulation of health data (Part II.C). In Part III, I will offer some concluding thoughts. First, however, I will provide a brief outline of the sources of privacy law and how it affects medical and other scientific research.

A. Sources of Modern Privacy Law

In the U.S., there is as yet no general federal privacy law. Federal privacy laws and regulations laws are sector-specific,[1] covering such areas as health (through the Health Insurance Portability and Accountability Act of 1996, or HIPAA)[2], finance (through the Gramm-Leach Bliley Act),[3] and online businesses that target children (Children's Online Privacy Protection Act, or COPPA).[4] In addition, the Federal Trade Commission is beginning to assert itself as a general regulator of privacy. There are also some federal criminal laws that have privacy implications (anti-hacking[5] and anti-

---

[1] *See* Ieuan Jolly, *Data Protection in the United States: Overview*, THOMAS REUTERS PRACTICAL LAW (July 1, 2017), https://content.next.westlaw.com/Document/I02064fbd1cb611e38578f7ccc38dcbee/View/FullText.html?contextData=(sc.Default)&transitionType=Default&firstPage=true&bhcp=1.

[2] HIPAA Privacy Rule, 45 C.F.R. § 160.

[3] Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act, 16 C.F.R. § 313.

[4] Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–05.

[5] *E.g.*, Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030.

wiretapping laws,[6] for instance), but these are beyond the scope of this discussion.

In the absence of a comprehensive federal privacy law, the states are the most important source of general privacy law. California has long been the leader, and remains so. Hence one piece of advice I often give to clients: comply with California law and you will usually be compliant in the other 49 states.

The development of international privacy law has been driven by the European Union, with other countries (except the U.S.) following its lead and adopting EU-style laws. The EU approach is fundamentally different from that taken in this country. The development of U.S. privacy statutes, both state and federal, has largely been motivated by a concern with the financial consequences of identity theft. Thus, most American laws protect "personally identifiable information," usually defined as a name, social security number, or the like that is linked to an account number or other financial identifier. In Europe, by contrast, privacy is treated as a fundamental human right—what Americans would think of as a constitutional right.[7] This is understandable, since there are millions of people in Europe with a living memory of storm troopers or secret police knocking on doors in the middle of the night and dragging people away. Consequently, EU privacy law is generally far more protective than American privacy law, protecting any kind of personal information, prohibiting any kind of intrusion on privacy or seclusion, and putting a much greater burden of compliance on businesses and other private actors (but not always on governments—think of the ubiquitous surveillance cameras that saturate the United Kingdom).

B. Four Waves of U.S. State Privacy Laws

State privacy laws have come in what privacy lawyers sometimes refer to as four waves. The first, toward the end of the last century, consisted of antihacking laws, both criminal and civil.[8]

---

[6] *E.g.*, Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510-22.

[7] *See, e.g.*, European Convention on Human Rights, art. 8, https://www.echr.coe.int/Documents/Convention_ENG.pdf.

[8] *E.g.*, CAL. PENAL CODE § 502 (West 2016).

The second, or "reactive" wave, led by a 2003 California law, required notification to potential victims of data security breaches.[9] The third, "proactive" wave (and my apologies to literate people everywhere for having to use that dreadful word), again stimulated by California legislation, requires that entities holding personally identifiable information use "reasonable security procedures and practices."[10] The fourth wave of state laws (also characterized as proactive),[11] which are in the process of being enacted, require such specific security measures as encryption and physical and technical controls.[12] A parallel development is that California and other states are moving into the health sector with privacy requirements that may be more onerous than those imposed by HIPAA.[13]

It is important to emphasize two other things about these state laws. First, unless specifically preempted, or displaced, by a federal law like HIPAA, the prudent assumption is that they will apply to medical and other scientific research in addition to any relevant federal law.[14] Second, many of them apply to all kinds of data media, from paper records to the cloud.[15] In fact, there is little privacy law anywhere that relates specifically to the cloud, so cloud-using researchers must try to adapt the existing rules to that environment.

C. Research-Related U.S. Federal Privacy Laws

1. HIPAA

The HIPAA Privacy Rule limits unauthorized use of personally identifiable health information to care-related activities by providers

---

[9] CAL. CIV. CODE § 1798.82 (West 2017). *See* generally Jolly, *supra* note 1.

[10] *E.g.*, CAL. CIV. CODE § 1798.81.5(c) (West 2016).

[11] *See* Julie Tower-Pierce, *Proactive State Privacy Laws Change Security Focus to Prevention*, TechTarget (Feb. 2009), http://searchsecurity.techtarget.com/magazineContent/Proactive-state-privacy-laws-change-security-focus-to-prevention.

[12] *E.g.*, 201 MASS. CODE REGS. § 17 (2009).

[13] *E.g.*, California Confidentiality of Medical Information Act, CAL. CIV. CODE §§ 56-56.37 (West 2000).

[14] HIPAA does not preempt state privacy laws that provide greater protection than it does. *See Does the HIPAA Privacy Rule Preempt State Laws?*, HHS.GOV (last visited July 26, 2013), https://www.hhs.gov/hipaa/for-professionals/faq/399/does-hipaa-preempt-state-laws/index.html.

[15] *E.g.*, N.C. GEN. STAT. § 75-65(a) (2009).

and their "business associates."[16] However, unauthorized r*esearch* use or disclosure is permitted, as long as the activity is approved by an Institutional Review Board. The use of de-identified health data is generally not restricted. Overall, HIPAA requires "reasonable and appropriate administrative, technical, and physical safeguards" in the handling of health data. Here, as elsewhere, federal law is technology-neutral, covering data media from paper to the cloud.

2. FTC Act

Under the New Deal-era Federal Trade Commission Act, the FTC has broad jurisdiction to prohibit and prevent "unfair or deceptive acts or practices."[17] The FTC has jurisdiction over all for-profit companies involved in interstate commerce, but not non-profits—a significant distinction for many research entities.[18] Until the last few years, the FTC's approach to privacy was simple: if you have an announced privacy policy, make sure you live up to it. More recently, however the FTC has begun to create and enforce substantive standards for privacy policies and practices, setting itself up as an all-purpose federal privacy regulator.[19] The new initiative focuses on "privacy by design," including reasonable efforts in data security, collection limits, data retention and disposal, and data

---

[16] 45 C.F.R. §§ 164.502(e), 164.504(e), 164.532(d)-(e) (2013). *See Business Associates*, HHS.GOV (last visited May 13, 2018), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html.

[17] 15 U.S.C. § 45(a) (2018). *See A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*, FTC (last updated July 2008), https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority.

[18] 15 U.S.C. §§ 44, 45(a) (2018). *See Opportunities and Challenges in Advancing Health Information Technology*: *Hearing Before the House Oversight and Government Reform Subcommittees on Information Technology and Health, Benefits, and Administrative Rules* 3 at n. 7 (2016) (statement of the Federal Trade Commission), https://www.ftc.gov/system/files/documents/public_statements/941063/160322commtestimonyhealthinfo.pdf.

[19] For a review of this history, see FTC STAFF, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS (Dec. 2010), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf.

accuracy.[20] The FTC's authority to enforce these standards has been upheld by a federal appellate court in the *Wyndham Hotels* case.[21]

The FTC has promised a collaborative, "soft-law" (best practices rather than rules) approach, but there are skeptics (including me).[22] The FTC issued a Privacy Framework report in March 2012 that fills in many details of its evolving standards and regulatory plans.[23] Even though non-profit research organizations are not subject to the FTC's jurisdiction, it would be prudent to assume that other regulators will look to the Privacy Framework for guidance in developing their own standards. Accordingly, it would make sense to treat the FTC framework as, at a minimum, a set of best practices to consult in shaping an organization's privacy program.

D. International Law: The EU Approach

Until May 25, 2018, the EU will continue to operate under its 1995 Data Protection Directive.[24] A Directive is a detailed standard that individual member countries must adopt through national legislation, a process that inevitably produces country-by-country variation.[25] Thus, compliance currently requires familiarity with both the directive and the national laws of the particular countries in which research data will be collected, processed, or stored. The new GDPR,[26] by contrast, will take effect automatically in all member countries.[27] It will perpetuate the Directive's core principles and requirements and will add a good deal more. Its specific implications for research are discussed below.

---

[20] *See FTC Issues Final Commission Report on Protecting Consumer Privacy: Agency Calls on Companies to Adopt Best Privacy Practices*, FTC (Mar. 26, 2012), https://www.ftc.gov/news-events/press-releases/2012/03/ftc-issues-final-commission-report-protecting-consumer-privacy.

[21] FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015).

[22] FTC STAFF, *supra* note 19 at i.

[23] *Id.* at 15.

[24] Council Directive 95/46/EC, 1995 O.J. (L 281) 31.

[25] *See Regulations, Directives and Other Acts*, EUR. UNION, https://europa.eu/european-union/eu-law/legal-acts_en (last visited Mar. 7, 2018).

[26] Regulation 2016/679, 2016 O.J. (L 119) (EU).

[27] *See Regulations, Directives and Other Acts*, EUR. UNION, https://europa.eu/european-union/eu-law/legal-acts_en (last visited Mar. 7, 2018).

The core features of the 1995 Directive include the following:

- It covers all "personal data": anything identifiable to a person.[28]
- Health-related and genetic data are always "sensitive," and thus subject to enhanced protection.[29]
- The burden of compliance is on the "controller"—the party that directs "processing," which includes collection, storage, transmission, or analysis of the data.[30]
- Consent of the data subject is generally required for any processing.[31]
- Processing must be for legitimate purposes and proportional to those processes.[32]
- The subject has rights of access, objection and opt-out.[33]
- The controller must ensure the security and integrity of the data.[34]

For American companies dealing in any kind of EU personal data, one of the most daunting aspects of the 1995 Directive is a set of rules concerning transferring personal data to non-EU countries.[35] These rules govern both intra-and inter-company transfers, and clearly apply to medical and scientific research data. Absent specific individual consent, transfer is generally forbidden unless the EU has certified the recipient country as providing EU-level privacy protection. The U.S. does not meet this standard, a problem that will persist under the GDPR. The following alternatives are available:[36]

1. The subject can give unambiguous consent to the transfer.

---

[28] Regulation 2016/679, *supra* note 26 at 33.
[29] *Id.* at 34. GDPR Recitals and Articles, recitals 34, 35, art 4.
[30] *Id.* at recital 18, arts. 2(b), (d)-(e).
[31] *Id.* at recital 31, art. 7(a).
[32] *Id.* at arts. 6(c), 7.
[33] *Id.* at arts. 10-14.
[34] *Id.* at arts. 6, 16-17.
[35] *Id.* at recitals 56-60, arts. 25-26.
[36] *See International Transfers*, EUROPEAN DATA PROT. SUPERVISOR, https://edps.europa.eu/data-protection/data-protection/reference-library/international-transfers_en (last visited Mar. 7, 2018).

2. The U.S. data importer can enter the EU-U.S. Department of Commerce Privacy Shield program, whereby a U.S company certifies that its policies and practices meet EU standards.[37] A predecessor program (the Safe Harbor) was invalidated by the Court of Justice for the European Union for providing inadequate protection against U.S. government snooping.[38] Because of this inadequacy, the CJEU held, the Safe Harbor violated the European Charter of Human Rights. The Privacy Shield is facing similar criticism, and the outcome is uncertain.[39] This Privacy Shield is not available to nonprofits because they are not subject to the FTC's jurisdiction.

3. The exporter and importer can use EU-approved contract terms ("model contractual clauses") between the data exporter and importer.[40] The parties must adopt the clauses without any modification whatsoever. The U.S. party must promise to provide EU-level protection, "respond" to EU mediation and "accept" the decision of a European national court. Because of these and other provisions, as well as their non-negotiability, the model contractual clauses are rarely acceptable to U.S. companies.

4. The U.S. data importer can do the same thing through "binding corporate rules."[41] The American company must amend its bylaws to adopt the EU principles and provide mechanisms for

---

[37] *See Privacy Shield Overview*, PRIVACY SHIELD FRAMEWORK, https://www.privacyshield.gov/Program-Overview (last visited Mar. 7, 2018).

[38] *See* Court of Justice of the European Union Press Release No 117/15, The Court of Justice Declares That the Commission's US Safe Harbour Decision Is Invalid (Oct. 6, 2015), https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf.

[39] *See* Julia Fioretti, *EU Regulators Threaten Court Challenge to EU-U.S. Data Transfer Pact* (Dec. 6, 2017, 6:37 AM), https://www.reuters.com/article/us-eu-dataprotection-usa/eu-regulators-threaten-court-challenge-to-eu-u-s-data-transfer-pact-idUSKBN1E01DP.

[40] *See Model Contracts for the Transfer of Personal Data to Third Countries*, EUR. COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en (last visited Mar. 7, 2018).

[41] *See Binding Corporate Rules*, EUR. COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/binding-corporate-rules_en (last visited Mar. 7, 2018).

ensuring compliance. This approach has been equally unpopular in this country.

A further concern of those doing research under the current Directive is the sheer complexity of the law. All medical data, and much other scientific research data, is characterized as "sensitive" and thus subject to the highest level of scrutiny and restriction. Since the Directive has been implemented at the national level, there is significant country-by-country variation in the laws and regulations pertaining to research.[42] Those national laws and regulations are, like the Directive itself, detailed and complex. Nonetheless, it has been possible for a non-EU research entity to simplify compliance for a multinational research project by creating an "establishment" (or place of business) in one country and centralizing the project there.[43] Many American researchers believe that the UK has offered the most research-friendly environment in which to set up an establishment (in addition to avoiding language barriers). With Brexit looming, of course, any predictions about this or any aspect of the EU-UK legal relationship are speculative.

Under current law, critical country-by-country regulatory variables include: whether the approval of the national Data Protection Authority (DPA) is required before collecting data; whether individual subject consent is necessary and, if so, what form of consent is sufficient in order to collect or export particular kinds of data; and whether de-identified or anonymized data is exempt from regulation.[44]

---

[42] *E.g.*, Directive 95/46/EC, *supra* note 24, at art. 2; *see* Gauthier Chassang, *The Impact of the EU General Data Protection Regulation on Scientific Research*, 11 ECANCERMEDICALSCIENCE 709 (2017), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5243137/.

[43] Directive 95/46/EC, *supra* note 24, at recital 19, art. 4.

[44] See Andrew Charlesworth, *Data Protection and Research Data: Questions and Answers*, JISC (2016), https://www.ukdataservice.ac.uk/media/604452/jisclegal-data-protection-and-research-data.pdf.

II. RECENT DEVELOPMENTS, INTERNATIONAL AND DOMESTIC

A. The EU GDPR

On April 14, 2016, the Parliament of the European Union gave final approval to the long-discussed GDPR, which will replace the current regime of country-by-country laws under the 1995 Data Protection Directive.[45] Whereas an EU Directive requires implementation by individual EU member states, the GDPR is a Regulation (much like a federal law in this country) that will take immediate effect in all EU countries on May 25, 2018.[46] This forthcoming unification of EU law will have both costs and benefits for researchers.

1. Key Features of the GDPR

As noted earlier, the GDPR builds on and expands the privacy protections provided by the current Directive. The key features of the GDPR include the following:

- The GDPR continues the broad definition of "personal data" to include any information from which a natural person can be identified.[47]

- In principle, the GDPR applies to all "controllers" and "processors" of EU residents' personal data, regardless of their location. A processor is anyone who collects, manipulates, uses, or stores personal data; a controller is a party that directs or controls processing. [48] Parties outside the EU are subject to jurisdiction if they offer goods or services to EU residents or monitor their behavior.[49]

- Personal data can be collected only for "specified, explicit and legitimate purposes" and can be processed only in ways that are compatible with those purposes.[50]

---

[45] Directive 95/46/EC, *supra* note 24.

[46] *Regulations, Directives and Other Acts*, EUR. UNION, https://europa.eu/european-union/eu-law/legal-acts_en (last visited Mar. 7, 2018).

[47] Regulation 2016/679, *supra* nota 26 at art. 4(1).

[48] *Id.* at art. 4(2), (7)-(8).

[49] *Id.* at arts. 2-3.

[50] *Id.* at recital 170, art. 5.

- In most cases, a controller must get specific, informed, and unambiguous affirmative consent to collect and process data; merely providing an opt-out right is insufficient.[51] "Explicit" consent is required for sensitive data, such as genetic or biometric data or data pertaining to health, sexuality, or political views. Subjects must be able to withdraw consent at any time and it must be as easy to withdraw consent as to give it.[52] Controllers bear the burden of being able to demonstrate consent upon demand by a DPA.[53]
- DPAs can fine violators up to 4% of gross revenues.[54]
- The controller is responsible for all aspects of processing and must be able to demonstrate compliance with law.[55]
- Subjects must be given free access to data within one month of a request.[56]
- Parental consent is usually required for subjects under age 16.[57]

2. The GDPR and Scientific Research

The GDPR has a number of provisions relating to health and other scientific research. In general, the collection, use, and transfer of data for research purposes will become more uniformly regulated, an improvement over the current patchwork of rules. However, the specific rules are complex and generally more onerous than under current law.[58] For example, "explicit" consent is required for sensitive data like health information, but it is not clearly defined.[59] More helpfully, scientific and other research receives some relief from the usual restrictions on collection and processing of data. For example, anonymous data—which is not identifiable to a human subject—is not subject to the GDPR at all,[60] while pseudonymous

[51] *Id.* at arts. 6-7.
[52] *Id.* at art. 9(2)(a).
[53] *Id.* at art. 7(1).
[54] *Id.* at art. 83(5).
[55] *Id.* at recital 74, arts. 30, 42(4), 83.
[56] *Id.* at art. 15.
[57] *Id.* at art. 18.
[58] *See id.* at recitals 159-62, arts. 5(b), 5(e), 9.
[59] *Id.* at art. 9(2)(a).
[60] *Id.* at recital 26.

data—which is not directly identifiable--is covered by the GDPR, but enjoys favored status.[61] In addition, there are some circumstances in which a research organization may—and I stress *may*—be able to collect and process data without consent.[62] In addition, obtaining broad informed consent from a research subject at the outset of a project may support more extensive processing than the Regulation would otherwise permit.[63] Overall, after some detailed preparation, researchers will probably find it easier to do research in EU than under the current law.

Sending data from the EU to the U.S. will remain a significant problem. Individual consent remains a valid basis for transfer.[64] Getting consent to transfer could presumably be part of obtaining informed consent to participate in the research. Absent consent, the available options continue to be new Privacy Shield,[65] the unpopular model contractual clauses,[66] and the even less popular binding corporate rules.[67]

Non-profits cannot participate in the Privacy Shield because the rules are enforced by the FTC and non-profits are not subject to its jurisdiction.[68] For eligible private companies, the substantive standards are similar to those under the former Safe Harbor, with heightened attention to GDPR principles. Important points of emphasis include the following:

---

[61] *Id.* at recitals 26-29, arts. 4(e), 25(1), 32(1)(a), 89(1).

[62] *See id.* at arts. 5(1)(b), 6(1)(e)-(f), 9(2)(j).

[63] *See id.* at recital 33.

[64] *Id.* at art. 49(1).

[65] *See Privacy Shield Program Overview*, PRIVACY SHIELD FRAMEWORK, https://www.privacyshield.gov/Program-Overview (last visited Mar. 7, 2018).

[66] Regulation 2016/679, *supra* nota 26 at arts. 46(2)(c)-(d), 93(2).

[67] *Id.* at art. 47.

[68] *See generally* PRIVACY SHIELD FRAMEWORK, https://www.commerce.gov /page/how-join-privacy-shield-guide-self-certification (last visited Mar. 7, 2018).

- Companies must self-certify their compliance to the U.S. Department of Commerce, [69] with annual renewal.[70]
- Companies must commit—in a published privacy policy—to greater transparency in data collection and handling.[71]
- Companies are fully responsible for the conduct of their third-party data service providers.[72]
- Companies must respond to EU citizen complaints within 45 days, provide a free alternative dispute resolution service, and agree to binding arbitration before a "Privacy Shield Panel" whose members are jointly selected by the Department of Commerce and the EU.[73]
- Companies transferring human resources data will be subject to the national DPAs in the EU countries where the data originates.[74]
- The U.S. Commerce Department has committed to vigorous enforcement, including referrals to national DPAs.[75]

---

[69] *How to Join Privacy Shield (Part 1),* PRIVACY SHIELD FRAMEWORK, https://www.privacyshield.gov/article?id=How-to-Join-Privacy-Shield-part-1 (last visited Mar. 7, 2018).

[70] *How to Re-certify to Privacy Shield,* PRIVACY SHIELD FRAMEWORK, https://www.privacyshield.gov/article?id=How-to-Re-certify-to-Privacy-Shield (last visited Mar. 7, 2018).

[71] *How to Join Privacy Shield (Part 1)*, *supra* note 69.

[72] *Accountability for Onward Transfer,* PRIVACY SHIELD FRAMEWORK, https://www.privacyshield.gov/article?id=3-ACCOUNTABILITY-FOR-ONWARD-TRANSFER (last visited Mar. 7, 2018); *Obligatory Contracts for Onward Transfers,* PRIVACY SHIELD FRAMEWORK, https://www.privacyshield.gov/article?id=10-Obligatory-Contracts-for-Onward-Transfers (last visited Mar. 7, 2018).

[73] *Recourse, Enforcement, and Liability*, PRIVACY SHIELD FRAMEWORK, https://www.privacyshield.gov/article?id=7-RECOURSE-ENFORCEMENT-AND-LIABILITY (last visited Mar. 7, 2018).

[74] *The Role of the Data Protection Authorities,* PRIVACY SHIELD FRAMEWORK, https://www.privacyshield.gov/article?id=5-The-Role-of-the-Data-Protection-Authorities-a-b (last visited Mar. 7, 2018).

[75] *Enforcement of Privacy Shield,* PRIVACY SHIELD FRAMEWORK, https://www.privacyshield.gov/article?id=Enforcement-of-Privacy-Shield, (last visited Mar. 7, 2018).

• The EU data subject will have a "right to erasure" in many cases, including with respect to childhood or sensitive data;[76] the CJEU has already found this to be a European fundamental human right.[77]

B. Common Rule Revision

1. From ANPRM to [Almost] Final Rule

On January 19, 2017, in one of its last official acts, the outgoing Obama administration issued a final revised version of the Common Rule—the regulation that governs the treatment of human subjects in all federally funded research.[78] This was the culmination of a process that began in 2011 when the Department of Health and Human Services (HHS) issued an Advance Notice of Proposed Rulemaking, or ANPRM, that envisioned major changes to the original 1991 Common Rule.[79] Then, on September 8, 2015, HHS and 15 other federal departments and agencies released a Notice of Proposed Rule Making (NPRM) that proposed specific changes to the Common Rule and opened a 90-day public comment period.[80] The NPRM's proposed changes would have greatly altered the rules for human subjects research, especially regarding biospecimens.

---

[76] Rita Heimes, *Top 10 Operational Impacts of the GDPR: Part 2 – The Mandatory DPO*, IAPP (Jan. 7, 2016), https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-2-the-mandatory-dpo/; *Compliance/Privacy*, APPSEC CONSULTING, https://www.appsecconsulting.com/compliance/data-privacy-gdpr-and-privacy-shield-compliance/ (last visited Mar. 7, 2018).

[77] Case C-131/12, Google Spain SL & Google Inc. v. Agencia Española de Protección de Datos (AEPD) & Mario Costeja González, 2014 E.C.R. 317 (May 13, 2014).

[78] *Revised Common Rule*, HHS.GOV (last edited Jan. 19, 2017), https://www.hhs.gov/ohrp/regulations-and-policy/regulations/finalized-revisions-common-rule/index.html; Federal Policy for the Protection of Human Subjects (Jan. 19, 2018), https://s3.amazonaws.com/public-inspection.federalregister.gov/2017-01058.pdf.

[79] HHS Announces Proposal to Improve Rules Protecting Human Research Subjects, HHS.GOV, https://www.hhs.gov/ohrp/regulations-and-policy/regulations/anprm-for-revision-to-common-rule/index.html (last visited Mar. 7, 2017).

[80] *Id.*

Among the most controversial of its proposals was the expansion of the definition of regulated "human subjects research" to include research using anonymous or deidentified human biospecimens.[81] This is a critical point because research that does not involve human subjects at all is not subject to the Common Rule's requirements. The comments from industry, research universities, and scientific and professional organizations were highly critical of some of the proposed changes.[82] There was an evident division between hard science (critical) and social science (anthropologists, for example); supportive commenters. Bioethicists were generally critical, but there were opinions on both sides.[83] Interestingly, the criticism of the NPRM did not follow partisan or ideological lines. With the exception of the bioethics community, just about everyone involved in research, from university medical centers to Big Pharma, opposed many of its provisions. There was a particularly withering critique of the biospecimen proposal from the National Academies of Sciences, Engineering, and Medicine, which argued that "continuing expansion of federal regulations on research is diminishing the effectiveness of the U.S. research enterprise."[84]

---

[81] *NPRM 2015 – Summary*, HHS.GOV, https://www.hhs.gov/ohrp/regulations-and-policy/regulations/nprm-2015-summary/index.html (last visited Mar. 7, 2017).

[82] COMMON RULE OVERVIEW, COUNCIL ON GOVERNMENTAL RELATIONS (Feb. 1, 2017), http://www.cogr.edu/sites/default/files/Summary%20of%20Changes%20to%20the%20Common%20Rule_COGR.pdf; Jenny Menikoff et al., *The Common Rule, Updated*, 376 N. Engl J. Med. 613, http://www.nejm.org/doi/full/10.1056/NEJMp1700736?query=TOC&; Scott Jaschik, *New 'Common Rule' for Research*, INSIDE HIGHER ED (Jan. 19, 2017), https://www.insidehighered.com/news/2017/01/19/us-issues-final-version-common-rule-research-involving-humans.

[83] Jocelyn Kaiser, *Update: U.S. Abandons Controversial Consent Proposal on Using Human Research Samples*, SCIENCE (Jan. 18, 2017, 4:15 PM), http://www.sciencemag.org/news/2017/01/update-us-abandons-controversial-consent-proposal-using-human-research-samples.

[84] *Congress Should Create Commission to Examine the Protection of Human Participants in Research; Notice of Proposed Rulemaking to Revise Common Rule Should Be Withdrawn*, NAT'L ACAD. OF SCIENCES, ENG'G, MED. (June 29, 2016), http://www8.nationalacademies.org/onpinews/newsitem.aspx?RecordID=21824.

The January 18, 2017 final version (the "Final Rule") adopted some of the changes proposed in the NPRM and dropped others, including the controversial expansion of the definition of "human subjects" to include non-identified biospecimens.[85] There have been numerous published summaries of the differences among the original Common Rule, the NPRM version, and the Final Rule.[86] Without trying to reinvent the wheel, here are some of the key provisions of the Final Rule that these sources point out. As just noted, the Final Rule does *not* expand the definition of "human subjects research" covered by the Common Rule to include research using anonymous or deidentified human biospecimens. At the same time, the Final Rule allows the use of "broad consent" from a subject for storage of and future research on identifiable biospecimens. The Final Rule states an intent to streamline and simplify informed consent documents, though it does add some additional elements—including, interestingly, whether biospecimens will be used for commercial gain. The Final Rule expands the categories of research that are "exempt" from Common Rule regulation because of their low risk profile—though, in something of an oxymoron, it provides that some of these exempt categories will now require limited review by an Institutional Review Board.

As it runs out, the Final Rule is still not final. Its "effective date" was to have been January 19, 2018. Responding to stakeholder complaints about the time needed to prepare and the lack of guidance from federal agencies, the Trump administration has postponed the "effective date and general compliance date" until July 19, 2018, with further delays possible.[87] Until then, researchers

---

[85] Federal Policy for the Protection of Human Subjects (Jan. 19, 2018), https://s3.amazonaws.com/public-inspection.federalregister.gov/2017-01058.pdf.
The official text of the Final Rule is a daunting 500-plus-page document. However, the complete text of the Final Rule appears at pp. 459-508, with an executive summary of the new provisions at pp. 360-362. The rest of the document consists of numerous tables (cost-benefit analyses and the like) required by law and a summary of and response to every public comment made in 2015.

[86] *Supra* note 82.

[87] This was done through a device called an Interim Final Rule issued jointly by all affected federal agencies. Federal Policy for the Protection of Human Subjects: Delay of the Revisions to the Federal Policy for the Protection of Human

should continue to follow the original Common Rule and apply only those provisions of the Final Rule that are consistent with the earlier rule.

2. Why Are Some Bioethicists Unhappy?

Several prominent bioethicists have criticized the Final Rule's failure to require informed consent for research on anonymous or deidentified human biospecimens. Hank Greely of Stanford has called it "a predictable result of the disparity in lobbying power" between the research and subject communities.[88] Another critic is Rebecca Skloot, the author of the best-selling book, *The Immortal Life of Henrietta Lacks*.[89] Lacks was a poor African-American woman who went to Johns Hopkins for treatment of cervical cancer, in the course of which some of her cancer cells were biopsied. Those cells—without her knowledge or consent—gave rise to the HeLa cell line which, directly and indirectly, has generated large amounts of money in which she and her descendants have never shared. A Lacks descendant has recently sued Johns Hopkins University in a belated effort to seek compensation. The suit faces many significant legal challenges, the biggest of which may be the statute of limitations.

Skloot and other critics of the Final Rule worry about three broad categories of harms to research participants: privacy-related, emotional, and financial.[90] On the privacy issue, Skloot has noted that Lacks ultimately lost her anonymity, and that she and her family endured the public disclosure of personal medical information.[91] That is likely to be an exceedingly rare event in the current research environment, regardless of how the Common Rule treats biospecimens. In fact, if I ask whether there a meaningful

---

Subjects, 83 Fed. Reg. 14 (Jan. 22, 2018), https://www.federalregister.gov/documents/2018/01/22/2018-00997/federal-policy-for-the-protection-of-human-subjects-delay-of-the-revisions-to-the-federal-policy-for.

[88] Kaiser, *supra* note 83.

[89] REBECCA SKLOOT, *The Immortal Life of Henrietta Lacks* (2010).

[90] Rebecca Skloot, *Your Cells. Their Research. Your Permission?*, N.Y. TIMES (Dec. 30, 2015), https://www.nytimes.com/2015/12/30/opinion/your-cells-their-research-your-permission.html.

[91] *Id.*

probability that someone will have the means and motive to reidentify my biospecimen, and then use that information to harm me, my answer is no.

Skloot has also drawn on the Lacks family's experience to catalogue the possible emotional harms, including "the shock of learning they were part of research" and being drawn into "debates over who controlled samples" and how those samples could be used.[92] I would not judge someone else's reaction to these consequences, but I would discount it by the current probability of similar things happening—and Skloot deserves much of the credit for bringing attention to the issue and thereby reducing that probability.

I think the most serious of these three concerns is the third, what Skloot has called "questions over profits."[93] A lot of people and institutions have made money from Henrietta Lacks's cells. She got none of it, and she was never told that the research was going on. The same thing has happened in a couple of other notorious cases, most infamously the 1990 California case of *Moore v. Regents of the University of California*.[94] This bothers me. If I am considering giving you a biospecimen and you think you might use it for money-making purposes, you should tell me. Some people might refuse your request outright; I would personally want the opportunity to negotiate for a piece of the action. Curiously—to me—the research and bioethics communities have almost uniformly rejected the ideas that an informed consent document is a contract and, especially, that money can be used as an inducement to contribute a research biospecimen (though they do approve of token payments as compensation for the subject's inconvenience).

A few years ago, several colleagues and I published two articles advocating a contractual model for biospecimen contributions to biobanks.[95] The key idea was a sliding scale of compensation: the

---

[92] *Id.*

[93] *Id.*

[94] 793 P.2d 479 (Cal. 1990).

[95] J. Conley, R. Mitchell, et al., *A Trade Secret Model for Genomic Biobanking*, 40 J.L. MED. & ETHICS 612 (2012); R. Mitchell, J. Conley, et al., *Genomics, Biobanks, and the Trade-Secret Model*, 332 SCIENCE 309 (Apr. 15, 2011).

more control over the sample that the subject ceded to the researcher, the more the subject would get paid. The reaction, in print and at conferences where we presented the papers, was very negative. Allowing subjects to treat their DNA as a commodity seemed to be viewed as unethical. I remember one anonymous journal reviewer—who advocated rejecting the article—writing that we had totally ignored the lessons of the Henrietta Lacks case. We thought that we had come up with a way to prevent the same thing from happening in the future. The lesson I took away from the whole experience was that, to our critics, the ethical principle of subject autonomy was little more than a rhetorical construct.

3. How Much Does the Final Shape of the Common Rule Really Matter?

At least with respect to research using biospecimens, the answer may be: not all that much. The reason is that many, many people are regularly consenting to the use of their biospecimens without ever becoming aware of it. I owe this realization to Jean Cadigan, a medical anthropologist at UNC Medical School, who co-teaches my Biotechnology and Life Sciences course at UNC Law School. In a class last year, Cadigan led us through a fascinating exercise about consent to research in teaching and research hospitals (most use very similar forms, so these comments could apply to almost any university medical center). First, she showed us an elaborate, carefully crafted informed consent video used by a university-affiliated biobank.[96] The biobank offers all the protections that the Common Rule requires and more. Then we looked at a specific consent for treatment form from the same university's hospital. By way of preamble, I should note that I and family members whom I have accompanied to various hospitals have had to sign this kind of document on several occasions in exigent circumstances. I have never read one—and I bet you have not either. We scribble our names on anything they put in front of us just to get the treatment started.

[96] I have chosen not to cite the forms—and thereby identify the hospital—discussed in the text. I have confirmed that these forms and policies are similar to those used by many other university research hospitals and biobanks.

But what would we find if we did read it? In the example we looked at, at the end of a long paragraph entitled "Consent for Use and Release of Information," I'd see that the patient gives the hospital permission "to release any information about me, my health, the health services provided to me . . . (4) as otherwise described in the Notice of Privacy Practices and as permitted by law." Then, if I dug up that Notice (as Jean did for our students), I'd find that the hospital (taking advantage of a HIPAA exception) asserts the right, "without [the patient's] authorization or an opportunity to agree or object," to use or disclose personal health information or "surplus specimens" (anything they take out of your body that they don't put back in) as long as "the use and/or disclosure relates to research." The bottom line appears to be that, however the Final Rule treats biospecimens, the research world will still be awash in unwittingly donated—and anonymized—tissue samples. This makes the anguish over the Final Rule, and the ethical aversion to our contractual model, seem like rearranging the deck chairs on the Titanic.

C. The FTC's Foray Into Health Privacy Regulation

In its July 29, 2016 decision in *LabMD, Inc.*,[97] the Federal Trade Commission clearly signaled its intent to get more involved in the regulation of health privacy. Specifically, the case indicates that the agency intends to go well beyond its traditional role of protecting consumers against deception and to begin scrutinizing the nuts and bolts of companies' health data security practices.

In most cases, the privacy of individually identifiable health information is protected by HIPAA's Privacy Rule, which is enforced by the Department of Health and Human Services. But HIPAA covers only data transactions between "covered entities" (providers, health plans, and health care clearinghouses) and their "business associates" (various kinds of service providers).[98] A lot falls through the HIPAA cracks, including the communication of

[97] LabMD, Inc., FTC File No. 102-3099, Docket No. 9357 (2016), https://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter. The case is now on appeal to the 11th Circuit, and oral argument was heard on June 21, 2017.

[98] *See supra* note 16.

individual patient information between treating physicians and testing laboratories, which is not covered by the HIPAA Privacy Rule. This is the gap that the FTC sought to fill.

As I noted above, one piece of news in this case is the FTC's move into the health privacy area. LabMD was in the clinical laboratory business from 2001 until 2014, when it suspended its testing business.[99] However, it has retained its previously collected patient samples and data and continues to provide past test results to providers. Therefore, one lesson to be drawn from the decision is that if you are in the health business but not covered by HIPAA, you cannot assume that you are unregulated—the FTC will be watching, even if no one else is, for as long as you keep individual health data.

The second piece of news is how far the FTC is going in its regulatory efforts. The agency has long claimed a mandate to regulate privacy under section 5 of the FTC Act, which authorizes it to police "unfair or deceptive acts or practices in or affecting commerce." Until the last few years, the FTC focused on the word "deceptive" in scrutinizing privacy practices.[100] It said, in effect, "we won't tell you what to do, but if you disclose a privacy policy to consumers, you have to live up to it"—to do otherwise would be deceptive. Now the FTC *is* telling you what you have to do.

In a series of more recent business cases (involving, for example, car dealers and hotels), the FTC has gone beyond posted privacy policies to take a close, substantive look at just what companies are doing to protect consumers' personal and financial information.[101] The agency is insisting that privacy and data security practices be *reasonable*, a loosely defined and evolving standard that seems to focus on industry best practices. The regulatory algorithm is that

[99] LabMD, Inc., FTC File No. 102-3099, Docket No. 9357 (2016), https://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter.

[100] *See supra* notes 17-23.

[101] See J. Conley & R. Bryan, *Practical Responses to Data Privacy Developments in the U.S. and EU*, 30(8) WESTLAW COMP. & INTERNET J. 1 (Sep. 21, 2012).

unreasonable privacy practices = unfair trade practices, and thus violate section 5.[102]

This is precisely the approach the FTC took in the case. Among the data security practices deemed unreasonable were: failing to use an intrusion detection system, neglecting to monitor file integrity or traffic coming across the firewalls, never deleting any data, and not training employees. One consequence of this inattention was that employees installed P2P file-sharing software that exposed thousands of health records to the outside electronic world.[103] *Exposed* is a key word here: there was no evidence of any actual data theft. The FTC found this irrelevant, however. Its decision relied on the rarely cited section 5(n) of the FTC Act, which provides that an act or practice can be held unfair if it "causes substantial harm to consumers." So the threat of harm can constitute substantial harm, and the absence of actual harm is no defense.

A couple of other legal issues in the case are worth mentioning. The first concerns the FTC's authority to judge the substantive adequacy of privacy practices, as opposed to merely ensuring that companies live up to their privacy policies. A number of FTC targets have challenged this authority, including LabMD, which asked both the FTC itself and two different federal courts to rule that the agency was going too far. Its requests were rejected, as has happened in every other case.[104] The leading case is *Wyndham Hotels*, where the U.S. Court of Appeals for the Third Circuit upheld the FTC's authority to regulate the substance of cybersecurity. A second point concerns remedies.[105] While the FTC has the power to fine offenders, it did not seek a monetary penalty against LabMD. Instead, it imposed (via injunction) detailed requirements for

---

[102] The most comprehensive—albeit somewhat dated—statement of the FTC's outlook can be found in its 2012 report on consumer privacy. *See* FTC STAFF, *supra* note 19, at 15.

[103] LabMD, Inc., FTC File No. 102-3099, Docket No. 9357 (2016), https://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter.

[104] *Id.*

[105] FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015).

improved security practices.[106] Prospective targets should not take much comfort from this: the agency *can* seek fines, and LabMD complained bitterly about the burden imposed by the injunction. One piece of good news for potential targets is that private parties cannot sue for violations of the FTC Act, although they may have comparable rights under similarly worded state "Little FTC Acts" (e.g., North Carolina's).[107]

Companies that collect, transfer, store, or use individual health information should therefore keep these points in mind:

- The fact that you are not a covered entity or business associate under HIPAA does not mean that you are free from federal regulation—the FTC is aggressively asserting its authority in the interstices of privacy law.
- The FTC clearly believes that in privacy and data security, unreasonable = unfair and is thus illegal.
- Reasonableness is a fluid and evolving concept, likely to be tied to best practices in a given industry.
- To get a more specific idea of what the FTC thinks is and is not reasonable in the health context, read the full *LabMD* decision carefully, paying close attention to the technical details. In designing your own practices, avoid LabMD's specific pitfalls, and whatever you do, do it better than LabMD did.
- The decision had no occasion to mention this, but the FTC does not have jurisdiction to regulate nonprofits. Someone else—including your state government—will, however, and the FTC's privacy standards are likely to provide a model for other regulators.

III. CONCLUDING THOUGHTS

The most accurate way—if not a very helpful way--to summarize the three developments discussed in this Essay is that health-related research is, from a legal perspective, getting both easier and harder. In the EU, the GDPR will provide a unified legal

---

[106] LabMD, Inc., FTC File No. 102-3099, Docket No. 9357 (2016), https://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter.

[107] N.C. Gen. Stat. §§ 75-1.1-45.

framework, with significant exemptions for research. However, the protections given to data subjects have been expanded, the consent requirements have been strengthened, and the potential penalties for noncompliance have been increased dramatically. In this country, the revised Common Rule should make it easier to do research with non-identifiable biospecimens, and to obtain consent for any kind of research. At the same time, new consent provisions are intended to make research projects more transparent to participants while imposing few new burdens on researchers. On the other hand, the FTC—expanding its role as a general privacy regulator—is extending its reach into health privacy, with implications that are yet unknown. The best advice to research organizations is to pay closer attention than ever to the changing legal and regulatory environment: if you do things right, you will enjoy greater autonomy and protection, but if you do things wrong, the consequences may be more severe.