Selling Health Data

De-Identification, Privacy, and Speech

BONNIE KAPLAN

Abstract: Two court cases that involve selling prescription data for pharmaceutical marketing affect biomedical informatics, patient and clinician privacy, and regulation. *Sorrell v. IMS Health Inc. et al.* in the United States and *R v. Department of Health, Ex Parte Source Informatics Ltd.* in the United Kingdom concern privacy and health data protection, data de-identification and reidentification, drug detailing (marketing), commercial benefit from the required disclosure of personal information, clinician privacy and the duty of confidentiality, beneficial and unsavory uses of health data, regulating health technologies, and considering data as speech. Individuals should, at the very least, be aware of how data about them are collected and used. Taking account of how those data are used is needed so societal norms and law evolve ethically as new technologies affect health data privacy and protection.

Keywords: confidentiality; health data privacy; health records; big data; data mining; pharmaceutical marketing; health data sale; de-identification; HIPPA; EU Data Protection Directive; *Sorrell v. IMS Health Inc.*; *R v. Department of Health, Ex Parte Source Informatics Ltd.*

Introduction

Widespread use of electronic patient record systems enables opportunities to improve healthcare through data sharing, secondary use, and big data analytics but also creates more opportunities for privacy violations, data breaches, and inappropriate uses. A 2011 U.S. Supreme Court case concerning selling prescription data for pharmaceutical marketing, *Sorrell v. IMS Health Inc. et al.*,[1] provides an occasion for examining issues related to privacy and the protection of health data. Although the legalities of this case involve unique features of U.S. constitutional law related to free speech, a similar case in the United Kingdom in 2000, *R v. Department of Health, Ex Parte Source Informatics Ltd.*,[2] points to the international nature of these issues. In that case, *Source Informatics*, which operates as a subsidiary of IMS Health Inc. in the U.K.,[3] wanted to sell pharmaceutical companies information on general practitioners' prescribing habits.

According to their website, "IMS Health is the world's leading information, services and technology company dedicated to making healthcare perform better." Operating in more than 100 countries, it processes more than 45 billion healthcare transactions annually, organizes information from 100,000 suppliers, and serves more than 5,000 healthcare clients globally. Throughout the 1980s, IMS Health developed online services to report on pharmaceutical sales and it purchased or

I am grateful for the thoughtful contributions to the panel I organized on the *Sorrell* case for the 2011 American Medical Informatics Association Annual Symposium and for comments on a very early draft of some portions of this article by Paul DeMuro, J.D., C.P.A., M.B.A., M.B.I., Oregon Health and Science University, Portland, Oregon; Kenneth W. Goodman, Ph.D., F.A.C.M.I., University of Miami, Miami, Florida; and Carolyn Petersen, M.S., M.B.I., Mayo Clinic, Rochester, Minnesota.

Cambridge Quarterly of Healthcare Ethics (2015), **24**, 256–271.

doi:10.1017/S0963180114000589

collaborated with companies engaged in related activities. By 1989, it was providing "laptop-based sales management service tools for pharmaceutical sales representatives in the US and Europe."[4] The fact that IMS Health Inc. was joined in the U.S. case by SDI, Source Healthcare Analytics (a subsidiary of what then was Wolters Kluwer Pharma Solutions), and the Pharmaceutical Research Manufacturers Association makes it even more obvious that aggregating and selling prescription and other health data is an international enterprise. Thus, the *Sorrell* and *Source* cases raise more general global concerns, including the following: appropriate use and secondary use of data for data mining, marketing, research, public health, and healthcare; data ownership; and patient and clinician data and privacy protection. Consequences related to these concerns may affect biomedical informatics, patient and clinician privacy, and regulation in ways this article explores, both in and outside the United States.

Throughout the article, I focus primarily on *Sorrell*. I also bring in the *Source* case, calling into question whether de-identification, on which U.S. and European privacy regulation rests, is sufficient for these purposes. After introducing *Sorrell* and the U.S. legal environment, I turn to ethical analysis, focusing first on problems of de-identification and then on the particularities of prescription data. I discuss drug detailing (marketing), commercial benefit from the required disclosure of personal information, clinician privacy and the duty of confidentiality, beneficial and unsavory uses of health data, regulating health technologies, and considering data as speech. Elsewhere I discuss additional ethical issues related to selling health data.[5,6,7] Throughout, I take the stance that individuals should, at the very least, be aware of how data about them are collected and used, and that how those data are used is crucial.

The U.K. *Source* Case

The *Source* case permitted pharmacy data to be sold without patient permission because they were "anonymized," that is, specified identifying information was removed, what in the United States is called "de-identification." Such disclosure was deemed not to be unfair to or to disadvantage the patient and, therefore, was not judged a breach of confidentiality by the pharmacist. The U.K.'s Court of Appeal based this opinion on a Federal Court of Australia decision, declaring that patient privacy was safeguarded because patient personal identities were concealed. It found that "a reasonable pharmacist's" conscience would not be troubled by this use of a patient's prescription, so confidentiality would not be breached. Thus, the case was decided on privacy grounds and the decision depended on whether selling de-identified prescription data meant that pharmacists violated their duty of confidentiality. The Court of Appeal held that processing anonymized data was not within the scope of the European Union Data Protection Directive and the U.K. Data Protection Act of 1998 based on it.[8] This meant that pharmacists could disclose anonymized patient data for whatever purpose they wished.[9]

Some interpreted the decision to suggest that whether releasing patient data without consent was a breach of confidentiality depended on context, which raised questions about the scope and basis of the duty of confidentiality. In this reading, the decision ignored not only some of the provisions of the EU Data Protection Directive (and, indeed, the European Court of Human Rights, in a later

case, took a more expansive view of privacy[10]) but also the distress that could be caused by releasing even anonymized personal data. It also undermined patients' expectations of privacy.[11,12]

The U.S. *Sorrell v. IMS Health* Case

The U.S. *Sorrell* case was different from U.K. *Source* case in that it was argued and decided as a speech case. Nevertheless, it often is understood as pitting privacy protection against free speech, and resolving the apparent conflict in favor of free speech. Scant attention was paid to pharmacists' duty of confidentiality.[13] Despite the U.S. legalities, like *Source*, the case brings out significant issues of values and rights related to personal health data. As the ability of both government and private organizations to collect and aggregate individually identified personal data has grown, privacy versus data as speech has become the focus of much legal debate that illuminates privacy and policy considerations relevant everywhere.

In the United States, health data collected for clinical care are governed by the U.S. Health Insurance Portability and Accountability Act (HIPAA) (discussed subsequently), whereas free speech case law is based on the First Amendment to the U.S. Constitution. Though this legal background is particular to the United States, examining it is helpful for thinking through the issues involved, especially as U.S. law shares characteristics with international legal tools and also because what happens in the United States affects markets and services worldwide.

In *Sorrell*, the U.S. Supreme Court struck down a Vermont law that restricted selling prescriber prescription data to use for marketing prescription drugs without prescriber consent.[14] The challengers of the Vermont law—IMS Health, other data aggregators, and the Pharmaceutical Research and Manufacturers of America—argued the case on free speech grounds. William H. Sorrell, in his role as the attorney general of the state of Vermont, defended the law on the grounds that restrictions on direct-to-physician pharmaceutical marketing (*detailing*) were justified to (1) "protect medical privacy, including physician confidentiality, avoidance of harassment, and the integrity of the doctor-patient relationship" and (2) achieve Vermont's policy objectives of "improved public health and reduced healthcare costs"[15] by reducing "overprescription of new drugs [and by] controlling costs by stemming practices that promote expensive, branded drugs over generics."[16] Vermont's announced intention to tip the marketplace of ideas against drug companies was the "fatal self-inflicted wound" for free speech.[17] The court, in a 6-3 decision, rejected Vermont's position and struck down the law.

The United States is unusual in its tradition of constitutional protection of speech. The First Amendment to the U.S. Constitution—"Congress shall make no law . . . abridging the freedom of speech"—has come to cover a wide range of forms of expression. Different categories of speech, related to their purpose and value, have developed and are protected differently. Generally, common business practices and expression that is part of economic activity, such as marketing, advertising, and contracts, have not been protected as speech, or, when they have been protected, they are protected differently from, for example, political speech or artistic expression.

Commercial speech, such as advertising, is regulated according to criteria in the 1980 Supreme Court decision *Central Hudson Gas & Electric Corporation vs. Public Service Commission of NY*.[18] In *Sorrell*, the court did not apply the

commercial speech standards of *Central Hudson* to strike down the Vermont statute. Instead, the majority opinion applied the heightened judicial scrutiny standard governing individual speech, declaring that "[s]peech in aid of pharmaceutical marketing . . . is a form of expression protected by the Free Speech Clause of the First Amendment."[19]

The *Sorrell* decision is ambiguous and can be considered a retreat from previous U.S. commercial speech doctrine, a defense of not singling out speech that is disfavored, or a judgment that all data are "speech" and so any data regulation is subject to U.S. constitutional protection. The data-are-speech argument has trumped the privacy argument in U.S. courts, where data traditionally have been considered speech.[20]

The *Sorrell* case received considerable attention because the decision involved constitutional issues of speech and privacy. Ironically, the court largely avoided issues of privacy.[21] The First Amendment implicitly protects aspects of privacy in the form of freedom of thought, intellect, and association—and, in the famous defining words of Justice Louis Brandeis, citing Judge Cooley, "the right to be let alone"[22]—though generally not privacy claims related to disclosing highly sensitive truthful personal information.[23] But the *Sorrell* case also concerns public health, healthcare, and regulatory policy as it relates to preserving both free speech and privacy—and healthcare data privacy.

Data De-Identification and Privacy

Both the *Source* and *Sorrell* cases assume de-identification serves to protect privacy. Indeed, the foundation of much privacy regulation is the idea that if there is no personally identifiable information, there is no privacy harm.[24] Making de-identification central to privacy raises significant ethical and legal concerns. Relying on de-identification assumes that patients mainly are concerned not to have their names attached to data about them. However, this is not always how they see it. Henrietta Lack's family was upset because her name was *not* attached to her cell line.[25] Individuals may object to using their personal data, de-identified or not, in research that they consider repugnant, for example, for contraception research, animal research, embryonic research, or genetic research. Patients who think it wrong that they themselves have no commercial interest in data about themselves, but that others do, may be distressed by practices they consider unethical by data aggregators, pharmaceutical companies, or individuals who sell patient data and so may not wish to contribute to these endeavors' profits.[26] Also at issue is who determines if data are identifiable. Whether an official, such as a data controller in the EU, can identify an individual is not the same as whether a marketer, newspaper reporter, neighbor, or other party could.[27] Pharmacists', physicians', nurses', or patients' experiences of breaches of confidentiality are, to them, violations regardless of what courts decide.

The conviction that de-identification results in anonymization that protects individual privacy also is problematic. It rests on the assumption that it is possible to create a static set of criteria that "identifies" an individual, regardless of context, individual preference, changes over time, or what else may be known or revealed about the person. As the information kept in medical records grows to include patients' genomes and other genetic and biometric information as well as data on social and behavioral determinants of health (such as smoking status, employment,

gender orientation, education level, ethnicity, and living conditions[28]), it will be easier to identify patients from their records. Furthermore, as data collection proliferates in all walks of life, technological developments and the computer science specialty of reidentification science are creating techniques to combine previously separate databases.[29] Despite considerable research also under way to combine patient information while protecting patient privacy,[30] currently, de-identification is insufficient,[31,32,33] making the basis for decisions that data can be anonymized, like that of the U.K.'s Court of Appeal in *Source*, suspect.

These considerations pertain to all health data privacy protection that depends on de-identification. The ability to combine databases makes reidentification easier, even if some of the databases contain only de-identified records. Relying on de-identification contributes to what has been called inadequate problematic legal frameworks for data protection via the European Data Protection Directive and U.K. law. Addressing the concerns "would require a significant shift in approach towards data-protection across Europe."[34] Similar deficiencies afflict U.S. law,[35] in which agencies as influential as the Institute of Medicine recognize that "the HIPAA Privacy Rule does not protect privacy as well as it should, and that, as currently implemented, it impedes health research."[36] Moreover, privacy protection depends not merely on de-identification, or even anonymization, but also on expectations, transparency, and how data are used.

HIPAA, however, does not apply to the *Sorrell* case. The reasons, discussed next, highlight further the need to revisit this sort of legislation, in the United States and elsewhere.

The U.S. Health Insurance Portability and Accountability Act (HIPAA)

Both U.S. law and EU data-protection policies make special note of health information. The European Union takes a comprehensive general approach to privacy, reflected in the 1995 Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.[37,38]

Unlike in European countries, where the EU Data Protection Directive takes an expansive view of privacy, in the United States there is no omnibus privacy law. Privacy protection is more limited and is governed differently in different sectors, resulting in what Europeans consider a "reluctance to protect patient medical data from misuse."[39] As new technological developments make widespread data collection and aggregation possible, increasing both the possibility and harms of disclosing sensitive data, U.S. laws are developing to address privacy. Health data are subject to myriad, possibly conflicting, and often confusing privacy protections that data about, for example, grocery purchases, are not.[40] The common law tort system and more recent U.S. legislation reflect citizens' concerns of vulnerability, stigmatization, embarrassment, and discrimination from the release of sensitive information. Different governmental units and jurisdictions attempt to balance privacy, personal and public health, research, professionalism, free speech, and even national security by regulating different aspects of health data collection, use, and privacy.

Overarching national protection is governed by the U.S. Health Insurance Portability and Accountability Act (HIPAA) of 1996, widely thought to protect patients' health data collected in routine delivery of clinical care. The HIPAA Privacy

Rule derives from the same fair information practices (FIPs) as inform the EU Data Protection Directive. Both rely on de-identification for privacy protection.[41,42] HIPAA governs what is involved in de-identification, reuse, the consent or authorization for the use of personal health information (PHI), and what responsibilities are required of different organizations and agencies. According to the Department of Health and Human Services, the law is intended to protect individuals' health information while providing for the sharing of that information to ensure quality care and for public health.[43] HIPAA was extended through the Privacy Rule put into practice in 2003 that placed limitations on the sale of medical information to third parties for marketing purposes. In ways that seem relevant to the *Sorrell* case, the Privacy Rule reflected concerns about marketing directed at encouraging patients to purchase or use a healthcare-related product or service.[44]

However, HIPAA does not apply to the *Sorrell* case, for three reasons. First, the Privacy Rule applies only to "covered entities"; their "business associates"; and, since the changes mandated by the 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act (part of the American Recovery and Reinvestment Act of 2009 [ARRA]), business associates' subcontractors—but not to other types of private businesses and public agencies. New and emerging organizations and actors are not enumerated in HIPAA and so are not governed by HIPAA requirements.[45] Only covered entities and their business associates "must obtain the individual's authorization to use or disclose PHI to create or make the marketing communication."[46] Doctors, for example, are not permitted to provide patient lists to pharmaceutical companies for those companies' drug promotions. However, contracts—such as the agreements patients click through when paying for medication or waivers they sign to allow their physicians to provide personal health information to their insurer—often allow disclosure of their personal health information. A 2007 study estimated that employers, insurers, the criminal justice system, and other parties obtain some 25 million authorizations for patient records as a condition of employment, insurance, or public benefits. Usually the entire record is sent; this practice has led to proposals to limit disclosure.[47]

Second, although de-identifying data (stripping data of HIPAA-specified identifying information) is a key part of HIPAA protection, individual authorization is not required to release de-identified patient data. The patient data in question in *Sorrell* were HIPAA de-identified.

Lastly, the case involved selling provider-identifiable prescription data, and clinicians' privacy is not protected by HIPAA—only patients' is. Thus, the sale of patient de-identified prescription data by data aggregators is HIPAA compliant. For these reasons and for others discussed subsequently, the *Sorrell* case highlights the need to examine health data privacy protections in light of the limitations of laws like HIPAA.

Ethical Issues

Legally, analyzing *Sorrell* involves considering whether marketing based on aggregated prescription data is protected as speech. In the United States, it is. However, as is evident in the discussion of *Source*, other concerns are involved. There are interwoven ethical issues related to (1) the extent to which de-identifying health data protects privacy; (2) selling healthcare data; (3) combining public and

private data; (4) clinician privacy, duty of confidentiality, and professionalism; (5) public health and healthcare costs; and (6) transparency, accountability, and consent.

What follows is an ethical analysis of these and related considerations. The discussion picks up from the privacy issues of *Source* to issues particular to prescription data and then flows to more general issues of health data privacy.

Ethical Issues—Drug Detailing

The Vermont statute cited the effects of pharmaceutical marketing to physicians, called "detailing," on clinical decisionmaking and professionalism, and the extent to which prescription writing is influenced by marketing practices.[48] *Source*, too, concerned selling data for detailing. Pharmaceutical detailing, it has been argued, raises significant public policy issues. Detailing can affect prescribing practices in potentially negative ways. Concerns include detailing's effects on safety, quality, efficacy, and cost.[49,50] Some argue that pharmaceutical detailing is fundamentally wrong and exploitative of professional relationships.[51] However, fault can lie on both sides: uninformed prescribing based primarily on marketing violates professional standards, and inappropriately influencing prescribers also is not ethical, even if it may be legal.

The costs of detailing can include the costs of prescribing medications that are more expensive than other options, the substantial costs of detailing itself, the costs of impaired care from not prescribing the most appropriate treatment, drug price increases presumed to result from aggressive marketing, and higher insurance premiums and prescription co-payments for more expensive drugs.[52,53,54,55] Detailing also can increase prescribing costs by influencing hospital formularies to include brand-name medications.[56] The amount spent on detailing essentially doubled from 1996 to 2004, steadily increasing each year (though it dipped in 2005).[57]

Detailing positively affects drug prices, as do other forms of advertising.[58,59] Those paying for drugs have an interest in reducing drug prices, though there are less heavy-handed ways to influence pricing than through such restrictions on detailing as Vermont's. Whether the money spent on this form of advertising could be better spent—the pharmaceutical industry spends about twice as much on marketing drugs to physicians (which includes detailing) as it does on research[60]—is a business decision, not one that should be legislated.

Seeing prescribers as uninformed and vulnerable in the face of pharmaceutical detailing seemed to be a factor in the Vermont legislation's intention to protect them. Whereas some physicians find detailers intrusive, others welcome them and the information they bring. In 2005, the average U.S. primary care physician interacted with detailers 28 times each week; the physicians reasoned that such interactions save time and better suit busy schedules than other ways of learning about drugs. Even though studies show that they may be influenced unduly by detailers in ways they do not recognize, physicians also understand the potential conflict of interest between marketing and patient care.[61] Enshrining in law negative views of prescribers as unable to make decisions about detailing or to resist sales pressure fundamentally wrongs them. There are other means to counteract the possible harms of directed detailing.

Selling Health Data

Ethical Issues—Required Disclosure—Others Profit

Issues of data disclosure are complicated when collecting data is required by law. Patients must provide personal information for treatment and medication. By law, many medications are available only with a prescription. By law, both prescribers and patients must be identified on prescriptions. By law, pharmacists dispense drugs, pharmacies are licensed, and they must collect and maintain prescription information that includes what medication was prescribed. The nature of a prescription itself can reveal private information about a patient's condition and a clinician's prescribing practices. When all this information was on paper, it was immensely difficult to collect data from different pharmacies to aggregate, process, and sell. Now it is easy and profitable, made easier because providing these data is a requirement for getting needed medications.[62] Patients have little choice, except perhaps in the choice of pharmacy, if they can find one that does not sell their data.

Data aggregators provide a valuable service and should be compensated for the value added by collecting, cleaning, and aggregating data, but the sources deserve some benefit as well. Currently, they may bear the primary costs. When data exist because they are required by law, marketing interests benefit from the legal requirements to collect data, while those required to provide and collect the information do not. This private benefit from a public mandate advantages some parties while potentially harming others.

Ethical Issues—Identifiable Data

It is unclear whether data aggregators receive patient-identifiable data.[63] Pharmacy data sold to data miners generally identifies the pharmacy, provider, and patient (including birth date and gender); the name, dosage, and quantity of the prescribed drug; and the date the prescription was filled.[64] Before removing identifying patient data, data aggregators add a so-called fifth P linking code to uniquely identify individuals each time they appear in the aggregator's database. The patient is de-identified, but longitudinal prescription data about that patient can be connected to the four Ps: product, prescriber, payer, and pharmacy. This unique patient ID enables patient tracking over time and, some have argued, could be used to link these data with data in public records (including hospital discharge databases) and commercial databases to reidentify patients, especially in sparsely populated areas.[65,66]

There also are concerns over combining data from private and government sources. In one telling example of this public-private connection, the Canadian Pension Plan Investment Board and TPG Capital purchased IMS Health in 2010. Another example involves Ontario's Diabetes Registry, operated by the government agency eHealth Ontario, which continually identifies patients newly diagnosed with diabetes and captures data such as laboratory values from existing databases. It is unclear whether these data for about one million identifiable Ontarians can be sold. Even though the Canadian Medical Association's Principles for the Protection of Patients' Personal Health Information of 2011 stipulates that "[p]atients should be informed that the treating physician cannot control access and guarantee confidentiality for an electronic health record," there has been little attention to protecting the privacy of personal health information kept electronically.[67]

Ethical Issues—Clinician Privacy

Clinicians' credentials and contact information are publicly available, but details about their practices and prescribing habits are not. Physicians are the archetype clinician; though clinicians other than physicians may prescribe, the focus has been on physicians, even though the same considerations would apply to all prescribers.

Vermont contended that few physicians knew that their prescription data were being sold.[68] Data aggregators combine prescription data with the Physician Master File of the American Medical Association (AMA). Few U.S. physicians may know of the AMA opt-out program (about 3 percent of prescribing physicians participate, according to a 2011 publication) for selling data, including the 80 percent of physicians who are not AMA members but whose data are sold nonetheless.[69] As of 2011, about 28,000 of the 650,000 practicing physicians opted out of the AMA's Physician Data Restriction Program (PDRP), launched in 2006 in response to a 2004 AMA survey showing that physicians thought intrusive drug detailing would be curtailed if their prescribing data were withheld.[70] The PDRP does not cover nonphysician prescribers, nor does it prevent data mining by pharmaceutical company employees other than sales representatives.[71] Furthermore, data mining companies may still collect and sell prescription information about those who opt out, though they are prohibited from providing it to marketers for three years.[72] At least in the United States, it is unlikely that legal protection of clinician privacy would be effective.[73] What may be done with data concerning physicians and clinicians needs more transparency and regulatory attention, whether in a private or in a public health delivery system.

Ethical Issues—Health Information Technology, Medical Devices, and Software Regulation: Speech, Regulation, and Property

How health data, and "speech" related to health and healthcare, are regulated in the large U.S. market can affect non-U.S. markets as well, just as EU restrictions on EU health data flow and processing outside the EU affect markets in countries that are not EU members. The *Sorrell* decision created concerns about how health data, health-related advertising, and product safety will, and should, be regulated. It treated data as speech. At issue in *Sorrell* was whether (1) transferring information from data mining companies to pharmaceutical companies or (2) speaking to prescribers to sell pharmaceuticals is speech or commercial activity. Judges deciding the *Sorrell* case had varying opinions,[74] similar yet better-crafted laws in some states have been upheld, and legal scholars debate the issue, suggesting an ethical issue where societal norms have yet to coalesce.

Common assumptions underlying privacy law and public attitudes are that speech and data are different, and that an individual's speech is different from that of a salesman or a company when promoting products. Exposing patients to potential privacy violations stemming from releasing their prescription data in the name of speech is disquieting. Selling patients' prescription data to those who will use them to sell pharmaceuticals to prescribers and patients is hardly popularly understood as a form of speech that should be protected.[75]

The *Sorrell* decision is one of a few cases to challenge U.S. privacy law on First Amendment grounds. In those few cases, lower courts treated communicating raw data as speech.[76] Even with the unusually strong free speech protections

afforded in the United States by the First Amendment, speech is not entirely free, and some speech is regulated. Governments around the world regulate healthcare and public health by balancing their value against individual liberties, sometimes to the detriment of individual liberty. In India, for example, public interest, welfare, and safety take precedence over individual rights, liberty, and autonomy; so privacy is judged on a case-by-case basis as an exception to the rule that permits government interference in private life.[77]

In the United States, such regulation includes mandating behavior to protect others (e.g., quarantines; vaccinations; and requiring disclosure of personal health information about, for example, sexually transmitted diseases or possible rabies transmission) and regulating advertisements (including advertising drugs and professional services) and other forms of speech. U.S. government agencies require warnings on cigarettes, restrict liquor sales, and regulate advertising claims by pharmaceutical companies. Thus, these regulations affect both individuals and commercial entities in ways that restrict freedom.

Because of *Sorrell*, and other recent cases, the court might be tending toward treating commercial speech as it does other speech. Although interpretations of *Sorrell* vary, health-related consumer protection regulations are expected to be challenged, continuing a trend toward a change of emphasis from the right of consumers to hear commercial information to the right of corporations to access potential customers even if doing so potentially is detrimental to health or public interest.[78,79,80,81] Already invalidated are U.S. Food and Drug Administration (FDA) restrictions on off-label marketing of drugs, graphic warnings on cigarette packages, and calorie disclosures in restaurants.[82] Following *Sorrell*, scholars and commentators predicted challenges to regulating the advertising and sale of cigarettes, alcohol, weight-loss products, and nutritional supplements and to FDA requirements that medical devices and drugs must be proven safe and effective.[83,84,85] With so large a U.S. market, challenges to FDA safety registries and device regulation have worldwide ramifications for automated devices, software, electronic health records, telehealth and mobile phone applications, embedded radio-frequency identification devices (RFIDs) and biometric chips, and other health information technologies.

Ethical Issues—Health Data: Speech or Property?

Some argue that treating data as speech facilitates knowledge creation and that data transfers enable access to information.[86] The *Sorrell* decision rightly states that "the creating and dissemination of information are speech. . . . Facts are, after all, the beginning point for much of the speech that is most essential to advance human knowledge and conduct human affairs."[87] Used rather differently than for marketing, big data analytics applied to prescription and healthcare data can increase knowledge of health, disease, and treatment, though selling big data could result in limiting data access and resultant knowledge to those who can pay.[88]

Access to information also relates to protecting property, including protecting intellectual property through patents and copyrights. Big data analytic procedures that include health data can be protected as intellectual property. However, intellectual property protection also can serve to prevent disclosure and transparency, rather than to enhance access to information. Software system contracts, including

those for electronic patient record systems, may be shielded as intellectual property.[89] The American Medical Informatics Association considers it unethical when this protection keeps key contract provisions concerning safety and conflict of interests secret.[90] This shielding also calls data ownership into question and certainly contravenes transparency. Law in and outside the United States does not address medical data ownership clearly; it is not clear who the owner should be, or whether personal ownership is better than the current approach.[91,92,93]

The idea of personal health data and medical information as property subject to commercial practices disturbs those who think it commodifies the self and sullies ideas of personhood. Commodifying this information also seems anathema to professional values and the special relationship between doctor and patient.[94,95] It seems even worse when patients do not know that commidification is occurring and when providers cannot easily use the records they generate to conduct research.

Conclusions

Ethical and policy analysis related to health data and informatics should take into account public expectations and also the benefits and harms of how the data are used. Individual liberties crosscut public and individual health issues. De-identification is becoming increasingly untenable as a means of protecting privacy when supposedly anonymized data can easily be combined with other identifying data. Conflicting interests related to privacy and to the need to exchange and mine data are complicated further in the United States by protection of speech, which includes commercial uses of data such as marketing based on prescription data. Although data sharing among healthcare providers for research purposes and for patient safety can improve quality of care, individuals concerned about the release of their data may withhold information that could benefit their care as well as skew data on which these quality improvements are based. Many patients do not know what is, or can be, done with data about them, and many would not object to having their data used for research or improving care, but keeping them ignorant is not the way to address potential concerns. In the United States, as elsewhere, the lack of legal accountability and poor public transparency about health data uses feed privacy concerns.[96] Secrecy also undermines the possibility of informed consent and violates the widely recognized rights of patients to know what information is being held about them and to correct and control how it may be used.

The *Sorrell* decision was based on U.S. constitutional free speech protections, not on privacy grounds, and not on health-related considerations concerning the growing use of health information databases, data sharing, data aggregation, and biometric identification. It could be argued that protecting public and individual health, and privacy, is more valuable than the liberty to analyze data in the service of marketing. Expanding "free speech" to encompass selling and using prescription data to sell pharmaceuticals to prescribers and patients seems to stretch the concept of free speech.[97] Yet, as the Supreme Court decided in this case, the state deciding which kind of speech is permitted and which data users are favored over others is detrimental to both personal freedom and the marketplace of ideas.

In the Information Age, it is popular to promote the view that information should be free. New ways to collect, store, combine, and disseminate personal information continue to develop. Just because it is possible to compile and distribute extensive dossiers of personal data far more easily than in the past does not mean this should be done. As law evolves, some speech and some data become protected and some lose protection, and some are valued differently from others. But whether or not data are speech, it matters how data are used, for what purpose, and by whom. Use can be regulated, as some data uses are. If data collection is required through legal mandate or to receive medical treatment, it should be neither illegal nor unethical to regulate its use. For other data, those closest to providing and generating them should know, and agree to, their use and should, in some way, benefit or be compensated for it. Societal norms as to how to achieve this will vary over time and place.

Ethical considerations regarding data use will, and should, evolve as cases like *Source* and *Sorrell* encourage debate over propriety and values related to different kinds of data use and data users. The legal decisions are problematic on a variety of grounds. Appropriate uses by appropriate users should be justifiable on better grounds than the speech arguments in cases like *Sorrell*. The issues involved provide an occasion to assess the scope of existing health information privacy protection and to consider how it should be governed, taking into account both the uses and users of the information. Some uses are more beneficial than others.[98,99]

Governments that have or are considering laws to regulate prescription and other health data sales and use need to grapple with these ethical issues, tensions between privacy and other considerations, and shifting norms. Much legal writing in this area relates to critiques of disclosing personal information, yet there are good reasons for some disclosure. Rigid rules can prevent good policy and wise legal decisions that take account of the kind of data, the uses to which they are put, the balancing of values involved, public opinion, and broad ramifications for public welfare. There is opportunity for new law that protects health, privacy, and other values while meeting ethical norms and allowing for future developments. Rigid, rule-based requirements also can reduce moral behavior, as compliance is seen as sufficient, a ceiling rather than a floor for proper behavior.[100] Though what is legal and what is ethical are not necessarily the same, they can be brought closer together. Through most of history, health privacy was a matter of the Hippocratic Oath and the common law tort system that allowed for interpretation on a case-by-case basis.[101] Even though privacy tort law is not very protective of medical information,[102] that flexibility in thinking may lead to more ethical practices than rigid regulations and legal maneuvering around them.

In light of new technologies and biometric and genomic identification, there is a growing need for research to protect privacy both technologically and legally so as to take account of the values inherent in free speech and personal freedoms, healthcare, commerce, research, and privacy—issues illuminated by the *Source* and *Sorrell* cases. The numerous crosscutting issues suggest that other areas of law, ethics, and social policy also can inform the related ethical and legal considerations. Informaticians, too, can add to the conversation. They have been considering issues such as appropriate secondary use of data, patient and clinician relationships in light of the growth of electronic health records, e- and mobile health, and health information exchanges for some time. Laudably, research is ongoing and seeks to provide technological ways to protect privacy while achieving the healthcare

and social benefits of electronically collecting and analyzing health-related data.[103] Combining legal and ethics scholarship with informaticians' expertise concerning judicious and ethical data collection and their technical knowledge of data aggregation and identification can contribute to more informed policies.

New developments require revisiting policies. As the *Sorrell* court noted: "The capacity of technology to find and publish personal information, including records required by the government, presents serious and unresolved issues with respect to personal privacy and the dignity it seeks to secure."[104]

Notes

1. *Sorrell v. IMS Health Inc. et al*, 131 S. Ct. 2653 (2011).
2. *R v. Department of Health, Ex Parte Source Informatics Ltd.*, [C.A. 2000] 1 All ER 786. See also *R v. Department of Health, Ex Parte Source Informatics Ltd. European Law Report* 2000;4:397–414.
3. Businessweek. *Company Overview of Source Informatics Limited*; available at http://investing.businessweek.com/research/stocks/private/snapshot.asp?privcapId=26078316 (last accessed 18 May 2014).
4. IMS Health. *About IMS Health*; available at http://www.imshealth.com/portal/site/imshealth/menuitem.051a1939316f851e170417041ad8c22a/?vgnextoid=7311e590cb4dc310VgnVCM100000a48d2ca2RCRD&vgnextfmt=default (last accessed 14 May 2014).
5. Petersen C, DeMuro P, Goodman KW, Kaplan B. *Sorrell v IMS Health:* Issues and opportunities for informaticians. *JAMIA (Journal of the American Medical Informatics Association)* 2013;20(1):35–7.
6. Kaplan B. How should health data be used? Using *Source* and *Sorrell v. IMS, Inc*. to think with about privacy, secondary use, and big data sales. *Cambridge Quarterly of Healthcare Ethics*; forthcoming.
7. Kaplan B. Health data privacy. In: Yanisky-Ravid S, ed. *Beyond Intellectual Property: The Future of Privacy*. New York: Fordham University Press; forthcoming.
8. Beyleveld D, Histed E. Betrayal of confidence in the Court of Appeal. *Medical Law International* 2000;4:277–311, at 280, citing p. 796 of *R v. Department of Health, Ex Parte Source Informatics Ltd.*, [C.A. 2000] 1 All ER 786.
9. Dunkel YF. Medical privacy rights in anonymous data: Discussion of rights in the United Kingdom and the United State in light of the *Source Informatics* cases. *Loyola of Los Angeles International and Comparative Law Review* 2001;23(1):41–80.
10. Srinivas N, Biswas A. Protecting patient information in India: Data privacy law and its challenges. *NUJS Law Review* 2012;5(3):411–24.
11. See note 8, Beyleveld, Histed 2000.
12. Taylor MJ. Health research, data protection, and the public interest in notification. *Medical Law Review* 2011;19(2):267–303.
13. See note 9, Dunkel 2001.
14. See note 9, Dunkel 2001.
15. See note 1, *Sorrell v. IMS* 2011, at 2653.
16. Mello MM, Messing NA. Restrictions on the use of prescribing data for the use of drug promotion. *New England Journal of Medicine* 2010;365(13):1248–54, at 1248, citing IMS Health, Inc v. Sorrell, 630 F.3d 263 (2nd Cir 2010).
17. Outterson K. Higher First Amendment hurdles for public health information. *New England Journal of Medicine* 2011;365(7):e13(1)–e(3), at e13(1).
18. *Central Hudson Gas & Electric Corporation v. Public Service Commission of NY*, 447 U.S. 564 (1980).
19. See note 1, *Sorrell v. IMS* 2011, at 2653.
20. Bambauer JR. Is data speech? *Stanford Law Review* 2014;66:57–120.
21. Bhagwat A. *Sorrell v IMS Health:* Details, detailing, and the death of privacy. *Vermont Law Review* 2012;36:855–80.
22. Warren S, Brandeis L. The right to privacy. *Harvard Law Review* 1890;4:193–201, at 194.
23. See note 21, Bhagwat 2012.
24. Schwartz PM, Solove DJ. PII problem: Privacy and a new concept of personally identifiable information. *New York University Law Review* 2011;86(6):1814–94.
25. Skloot R. *The Immortal Life of Henrietta Lacks*. New York: Crown; 2010.

26. See note 8, Beyleveld, Histed 2000.
27. See note 12, Taylor 2011.
28. Institute of Medicine. *Capturing Social and Behavioral Domains in Electronic Health Records: Phase 1*. Washington, DC: The National Academies Press; 2014.
29. Ohm P. Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA Law Review* 2010;57:1701–77.
30. Malin BA, El Emam K, O'Keefe CM. Biomedical data privacy: Problems, perspectives, and recent advances. *JAMIA (Journal of the American Medical Informatics Association)* 2013;20(1):2–6.
31. See note 29, Ohm 2010.
32. Rothstein MA. The Hippocratic bargain and health information technology. *Journal of Law, Medicine and Ethics* 2010; Spring:7–13.
33. Rothstein MA. Access to information in segmented electronic health records. *Journal of Law, Medicine and Ethics* 2012 Summer:394–400.
34. See note 12, Taylor 2011, at 303.
35. See note 29, Ohm 2010.
36. Institute of Medicine. *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research*. Washington, DC: National Academies; 2009.
37. European Union. *EU Directive 95/46/EC—The Data Protection Directive*; available at http://www.dataprotection.ie/docs/EU-Directive-95-46-EC--Chapter-2/93.htm (last accessed 23 Mar 2014).
38. European Union. *The European Data Protection Supervisor*; available at http://europa.eu/about-eu/institutions-bodies/edps/index_en.htm (last accessed 23 Mar 2014). Maintained or enhanced in http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52012PC0011:en:NOT (last accessed 23 Mar 2014).
39. See note 9, Dunkel 2001, at 44.
40. See note 7, Kaplan forthcoming.
41. See note 29, Ohm 2010.
42. Koontz L. What is privacy? In: Koontz L, ed. *Information Privacy in the Evolving Healthcare Environment*. Chicago: Healthcare Information and Management Society (HIMSS); 2013:1–20.
43. United States Government, Department of Health and Human Services, Office for Civil Rights. *Summary of the HIPAA Privacy Rule*; available at http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/ (last accessed 30 June 2013).
44. See note 42, Koontz 2013.
45. McGraw D. *Privacy and Information Technology*. Washington, DC; 2009; Paper 25, O'Neill Institute Paper; available at http://www.law.georgetown.edu/oneillinstitute/research/legal-solutions-in-health-reform/Privacy.cfm (last accessed 1 July 2014) and http://scholarship.law.georgetown.edu/ois_papers/25 (last accessed 17 July 2014).
46. The Standards for Privacy of Individually Identifiable Health Information; available at http://aspe.hhs.gov/admnsimp/final/pvcguide1.htm (last accessed 19 Jan 2014).
47. Rothstein MA, Talbot M. Compelled authorizations for disclosure of health records: Magnitude and implications. *American Journal of Bioethics* 2007 Mar;7(3):38–45.
48. Vt. Stat. Ann. Tit. 18 §§4631d (Supp. 2010).
49. Findlay SD. Direct-to-consumer promotion of prescription drugs: Economic implications for patients, payers and providers. *PharmacoEconomics* 2001;19(2):109–19.
50. Gostin LO. Marketing pharmaceuticals: A constitutional right to sell prescriber-identified data? *JAMA* 2012;307(8):787–8.
51. Orentlicker D. Prescription data mining and the protection of patients' interests. *Journal of Law, Medicine and Ethics* 2010; Spring:74–84.
52. Curfman GD, Morrissey S, Drazen JM. Prescriptions, privacy, and the First Amendment. *New England Journal of Medicine* 2011;364(21):2053–5.
53. Hartung DM, Evans D, Haxby DG, Kraemer DF, Andeen G, Fagnan LJ. Effect of drug sample removal on prescribing in a family practice clinic. *Annals of Family Medicine* 2010;8(5):402–9.
54. See note 49, Findlay 2001.
55. See note 51, Orentlicker 2010.
56. Gooch GR, Rohack JJ, Finley M. The moral from *Sorrell:* Educate, don't legislate. *Health Matrix* 2013;23(1):237–77.
57. Donohue JM, Cevasco M, Rosenthal MB. A decade of direct-to-consumer advertising of prescription drugs. *New England Journal of Medicine* 2007;357:673–81.

58. de Frutos MA, Ornaghi C, Siotis G. Competition in the pharmaceutical industry: How do quality differences shape advertising strategies? *Journal of Health Economics* 2013;32:268–85.
59. See note 49, Findlay 2001.
60. Boumil MM, Dunn K, Ryan N, Clearwater K. Prescription data mining, medical privacy and the First Amendment: The U.S. Supreme Court in Sorrell v. IMS Health Inc. *Annals of Health Law* 2012;21:447–83.
61. See note 56, Gooch et al. 2013.
62. See note 8, Beyleveld, Histed 2000.
63. Atherley G. The public-private partnership between IMS Health and the Canada Pension Plan. *Fraser Forum* 2011:5–7.
64. See note 52, Curfman et al. 2011.
65. Joint Appendix, Vol. 1, at 155, *William H. Sorrell et al. v. IMS Health Inc. et al.*, 2010 U.S. Briefs 779 (2nd Cir. 2011) (No. 10–779).
66. Brief for the *New England Journal of Medicine*, the Massachusetts Medical Society, the National Physicians Alliance, and the American Medical Students Association as *amici curiae* supporting petitioners, *William H. Sorrell v. IMS Health Inc. et al.*, 2010 U.S. Briefs 779 (No. 10–779), 2011 U.S. S. Ct. Briefs LEXIS 299.
67. See note 63, Atherley 2011, at 7, quoting the Canadian Medical Association.
68. Data mining case tests boundaries of medical privacy. *CMAJ* 2011;183(9):E509–E10.
69. See note 52, Curfman et al. 2011.
70. See note 56, Gooch et al. 2013.
71. See note 5, Petersen et al. 2013.
72. See note 68, Data mining case tests boundaries of medical privacy 2011.
73. See note 56, Gooch et al. 2013.
74. See note 51, Orentlicker 2010.
75. Piety TR. *Brandishing the First Amendment: Commercial Expression in America*. Ann Arbor: University of Michigan Press; 2012.
76. See note 20, Bambauer 2014.
77. See note 10, Srinivas, Biswas 2012.
78. See note 17, Outterson 2011.
79. See note 21, Bhagwat 2012.
80. Mermin SE, Graff SK. The First Amendment and public health, at odds. *American Journal of Law and Medicine* 2013;39:298–307.
81. Tien L. Online behavioral tracking and the identification of Internet users. Paper presented at: From Mad Men to Mad Bots: Advertising in the Digital Age. The Information Society Project at the Yale Law School. New Haven, CT; 2011.
82. See note 81, Tien 2011.
83. See note 16, Mello, Messing 2010.
84. See note 17, Outterson 2011.
85. See note 75, Piety 2012.
86. See note 20, Bambauer 2014.
87. See note 1, *Sorrell v. IMS* 2011, at 2667.
88. Pasquale F. Restoring transparency to automated authority. *Journal on Telecommunications and High Technology Law* 2011;9:235–54.
89. Koppel R, Kreda D. Healthcare information technology vendors' "hold harmless" clause: Implications for patients and clinicians. *JAMA* 2009;301(12):1276–8.
90. Goodman KW, Berner E, Dente MA, Kaplan B, Koppel R, Rucker D, et al. Challenges in ethics, safety, best practices, and oversight regarding HIT vendors, their customers, and patients: A report of an AMIA special task force. *JAMIA (Journal of the American Medical Informatics Association)* 2011;18(1):77–81.
91. Evans BJ. Much ado about data ownership. *Harvard Journal of Law & Technology* 2011;25(11): 70–130.
92. See note 6, Kaplan forthcoming.
93. See note 7, Kaplan forthcoming.
94. See note 63, Atherley 2011.
95. Hall MA, Schulman KA. Ownership of medical information. *JAMA* 2009;301(12):1282–4.
96. McGraw D. Building public trust in uses of Health Insurance Portability and Accountability Act de-identified data. *JAMIA (Journal of the American Medical Informatics Association)* 2013;20(1): 29–34.

97. See note 75, Piety 2012.
98. Miller RA, Schaffner KF, Meisel A. Ethical and legal issues related to the use of computer programs in clinical medicine. *Annals of Internal Medicine* 1985;102:529–36.
99. Goodman KW. Health information technology: Challenges in ethics, science and uncertainty. In: Himma K, Tavani H, eds. *The Handbook of Information and Computer Ethics*. Hoboken, NJ: Wiley; 2008:293–309.
100. White R. *Electronic Health Records: Balancing Progress and Privacy*; 2012 June 19; available at http://thehastingscenter.org/Bioethicsforum/Post.aspx?id=6907&blogid=140 (last accessed 29 June 2014).
101. See note 20, Bambauer 2014.
102. Abril PS, Cava A. Health privacy in a techno-social world: A cyber-patient's bill of rights. *Northwestern Journal of Technology and Intellectual Property* 2008; Summer;6(3):244–77.
103. See note 30, Malin et al. 2013.
104. See note 1, *Sorrell v. IMS* 2011, at 24.