5-1-2013

From FTC to HHS Regulation of Reputational Intermediaries' Use of Health-Inflected Data

Brian Glicos

From FTC to HHS Regulation of Reputational Intermediaries' Use of Health-Inflected Data

By: Brian Glicos

Table of Contents

I. INTRODUCTION

Advances in technology and the budding market for health information have lead to an increasing potential for abuse and even harm to an individual and his or her privacy. Ideally, the computerization of health records facilitates and promotes communications between health care providers. The expected result of the shift in recent years is to increase the quality of care provided by improving the efficiency with which information can be accumulated, processed and communicated. In reality, the change from paper records to electronic has brought to light gaps in the current statutory and regulatory framework, absence of clear ruling and misunderstanding of the potential dangers that lurk in the shadows of the secondary health information market.

The federal right of privacy to be discussed further arises from federal statute. The primary statute applicable to the health care privacy context is HIPAA.[1] To account for the advances in technology and advances in the arsenal of abusers of the technology, Congress should amend the Health Insurance Portability and Accountability Act ("HIPAA") to cover reputational intermediaries as "covered entities". States have tried unsuccessfully to protect health patients and those patients' individual health information via regulation and state statutes.[2] If a state is to act in the future, it must do so in a manner that fits within the narrow guidelines set forth by the Supreme Court's majority decision in *Sorrell v. IMS* (cite).[3] If left to the control of reputational intermediaries[4] the security of individual consumer's personal health information ("PHI") is at risk. Under the current regulatory scheme, most consumers have little to no knowledge that massive profiles exist that encompass nearly every aspect of the individual's

[1] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified in scattered sections of 42 U.S.C.)
[2] Sorrell v. IMS Health Inc., 131 S.Ct. 2653 (2011)
[3] Id.
[4] This paper focuses primarily on firms like Acxiom and IntelliScripts as prime examples of how reputational intermediaries take advantage of consumers and the lack of regulatipprofit.profit.

health and habits. Even if they know that the files exist, they can do little to prevent or direct the sale, use, misuse and abuse of access to the information. As a result, Congress' should devise an amendment to HIPAA and the amendment should include an accounting of when their information is disclosed (especially to entities outside the individual's health care provider); a private right of action for violation under the statute and should consider a provision that requires the individual's informed consent to sell the profile.

No regulatory framework is perfect but the one that is in place at the current time is simply inadequate. The computerization of health information is an idea motivated by the improvement of health quality. Included in the assessment of health care quality is how the care is being delivered, tracked and transferred. The consumer's knowledge of the care and how their records are being maintained should also be an aspect of that quality that Congress begins to pay more attention to. Increasing consumer knowledge of the markets that exist, the methods that are used and the potential abuses that occur help prevent consumer fraud; ethical dilemmas discussed herein and generally increase the efficiency and quality of health care the consumers are receiving.

II. THE PROBLEM: Privacy Threats: They Know What's In Your Closet

In 2008, Chad Turhune published just one example of how the unregulated market for consumer health information is a dangerous and unreasonably invasive industry. "Privacy and consumer advocates warn the information can easily be misinterpreted or knowingly misused. At a minimum, the practice is adding another layer of anxiety to a marketplace that many consumers already find baffling," Turhune wrote. He quoted independent insurance agent in Overland Park, Kansas Jay Horowitz saying, "and it's making it harder to find insurance for

people."[5] Isn't it troubling that an insurance company can reject applicants based solely on the individual's record of prescription medication without the opportunity to dispute or explain the record?

Walter and Paula Shelton of Gilbert, Louisiana were placed in that very situation when they applied for insurance from Humana, a large insurer in Louisville, Kentucky.[6] "They were rejected by the large Louisville insurer after a company representative pulled their drug profiles and questioned them over the telephone about prescriptions for Walter and his wife for blood-pressure and anti-depressants."[7] Where consumers like Walter and Paula are confronted with this information the natural reaction is to provide explanation for why the individual's prescription record should not preclude their ability to obtain insurance. Walter tried to explain that his wife had been prescribed blood-pressure medicine as an anti-inflammatory for her swollen ankles, and she had been prescribed anti-depressant medication as a sleep aid. At the time, both were considered common "off-label" treatment (especially the latter for menopausal women).[8] Walter pleaded with the Humana insurance representative to no avail, as both Walter and Paula were denied coverage and were uninsured at the time the article was written in 2008.[9]

The dangers are potentially severe and the concerns are understandable for consumers like Walter and Paula. They do not know if there is something in their prescription history, or some other form of data that has been collected, that can and will be used against them when applying for insurance coverage. Furthermore, the practice is unnerving because the consumer/patient is being penalized for taking medication that was likely prescribed by their

[5] http://www.businessweek.com/stories/2008-07-22/they-know-whats-in-your-medicine-cabinet
[6] Id.
[7] Id.
[8] Id.
[9] Id.

treating doctor. It causes unfair consequences to punish a patient for taking prescribed medicine without informing them that their decision to take the medication may or may not preclude them from gaining insurance coverage in the future. If insurers are using the data to deny coverage, it leads to a logical inference that they are also using the data to estimate costs for applicants. Few consumers have much knowledge of the insurance market, and it is unlikely that many have the wherewithal to recognize when and why their premiums are being increased for reasons unknown to the average customer. At the very least, one should be informed that their prescription record can be acquired by insurance companies and may cause hesitation and investigation when the consumer applies for coverage. The purpose of the health care reform supported by President Obama's administration is to improve access to and the delivery of health care services for all individuals, particularly low income, underserved, uninsured, minority, health disparity, and rural populations.[10] That purpose is sabotaged by the routine practice of denying applicants on the basis of what may be unreasonable assumptions guided by records with no room for explanation or dispute. "Most consumers and even many insurance agents are unaware that Humana, UnitedHealth Group, Aetna, Blue Cross plans, and other insurance giants have ready access to applicants' prescription histories."[11]

Some of the potential problems posed by the existence and accessibility of massive consumer profiles were discussed by Preston N. Thomas in Little Brother's Big Book: The Case for a Right of Audit in Private Databases. "Whoever controls our data can decide whether we can get a bank loan, on an airplane or into a country. Or what sort of discount we get from a merchant, or even how we're treated by costumer support. A potential employer can, illegally in

[10] PATIENT PROTECTION AND AFFORDABLE CARE ACT, PL 111-148, March 23, 2010, 124 Stat 119

[11] http://www.businessweek.com/stories/2008-07-22/they-know-whats-in-your-medicine-cabinet

the U.S., examine our medical data and decide whether or not to offer us a job."[12] Thomas agrees that there exists an obvious potential for harm and acknowledged that the current framework for keeping the harms in check is flawed and inadequate.[13] "Many of America's most important privacy protections do not apply to commercial data brokers… and they [data brokers] are generally unknown to society as a whole.[14]

a. Medical Records Are Regulated by HIPAA

The Health Insurance Portability and Accountability Act ("HIPAA") was passed on August 21, 1996 as part of Congress' response to the need for wide-reaching reform of the health care industry.[15] Subtitle F of Title II of HIPAA is entitled "Administrative Simplification," and states as its purpose to "improve the Medicare program under title XVIII of the Social Security Act, the medicaid program under title XIX of such Act, and the efficiency and effectiveness of the health care system, by encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information." [16] HIPAA focuses on the continuous transition to electronic health information.

---

[12] Id. *Citing, e.g.*, Bruce Schneier, *Our Data, Ourselves*, WIRED, May 15, 2008, http:// www.wired.com/politics/security/commentary/securitymatters/2008/05/securitymatters_ 0515 [hereinafter *Our Data, Ourselves*]; 153 CONG. REC. S1635-38 (daily ed. Feb. 6, 2007) (statements of Sens. Specter & Feingold) (introducing the Personal Data Privacy and Security Act of 2007).

[13] "As evidenced by the staggering depth and breadth of largely unregulated data collection, the current legal regime is inadequate for the task of addressing the complex relationship between an individual, his or her information, and the company that holds it. Id.

[14] Id. *Citing Nicole Duarte, Commercial Data Use by Law Enforcement Raises Questions about Accuracy, Oversight, CARNEGIE-KNIGHT INITIATIVE ON THE FUTURE OF JOURNALISM EDUCATION, Aug. 16, 2006, http:// newsinitiative.org/story/2006/08/16/commercial_data_use_by_law.*

[15] 194 A.L.R. Fed. 133 (2004)

[16] HIPAA § 261; 110 Stat. 2021; 42 U.S.C.A. § 1320d note. This subtitle consists of §§ 261 through 264 of the Act. Section 262 amends Title XI of the Social Security Act, 42 U.S.C.A. §§ 1301 et seq., to add a Part C, entitled "Administrative Simplification," with sections 1171 to

Congress authorized the Department of Health and Human Services (HHS) to promulgate regulations. [17] Collectively, the regulations are known as "The Privacy Rule".[18]

The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information (PHI), and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.[19] The regulations define PHI as information that:

> (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
> (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
> (i) That identifies the individual; or
> (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.
> The Privacy Rule requires covered entities to take the following actions with regard to protected health information:
> (1) Provide individuals with notice and certain rights regarding their protected health information;
> (2) Limit the use and disclosure of protected health information;
> (3) Obtain authorization from an individual to use or disclose protected health information;
> (4) Contract with service providers to provide assurances regarding proper use, appropriate disclosure and appropriate safeguards;
> (5) Implement policies and procedures to protect protected health information including: appointing a privacy officer, training the

---

1179, codified at 42 U.S.C.A. § 1320d through § 1320d–8. Section 263 amends the Public Health Service Act, at 42 U.S.C.A. § 242k(k).

[17] 45 C.F.R. § 160 et. seq.

[18] Id.

[19] http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html

> Business Associate's workforce, implementing safeguards and a complaint process.
> The Privacy Rule also permits limited uses and disclosures of protected health information, including disclosures to the patient and disclosures and uses related to payment, treatment, and health care operations.[20]

Under Health Insurance Portability and Accountability Act, the general rule pertaining to the disclosure of protected health information is that a covered entity may not use or disclose protected health information without a written authorization from the individual or, alternatively, the opportunity for the individual to agree or object.[21] However, HIPAA's provisions prohibiting disclosure of individually identifiable health information did not create private cause of action; the statute did not contain any language conferring privacy rights upon specific class of persons, but rather focused on regulating persons with access to individuals' health information, and HIPAA merely created specific means of enforcing the statute.[22] HIPAA's coverage is limited to "covered entities", which is a term defined by section 160.103 of title 45, Code of Federal Regulations as "health plans, health care clearinghouses and health care providers who transmit any health information in electronic form in connection with health care transactions covered by HIPAA."[23] Thus, HIPAA does not prohibit non-covered entities from disclosing protected health information (PHI), furthermore, there are exceptions that permit covered entities to disclose PHI without obtaining the authorization from the patient first.[24]

---

[20] Christopher R. Smith (FNd1), Somebody's Watching Me: Protecting Patient Privacy in Prescription Health Information, 36 Vt. L. Rev. 931, 948-49 (2012)
[21] Health Insurance Portability and Accountability Act of 1996, § 101(a) et seq., 42 U.S.C.A. § 1181 et seq.; 45 C.F.R. §§ 164.508, 164.510. Isidore Steiner, DPM, PC v. Bonanni, 292 Mich. App. 265, 807 N.W.2d 902 (2011).
[22] Social Security Act, § 1177(a), as amended, 42 U.S.C.A § 1320d–6(a). University of Colorado Hosp. v. Denver Pub. Co., 340 F. Supp. 2d 1142 (D. Colo. 2004).
[23] 45 C.F.R. §§ 160.103
[24] 45 C.F.R. §§ 164.501

b. Reputational Intermediaries Are Not Covered by HIPAA

As a result of the narrow scope of HIPAA's Privacy Rule, Firms like Acxiom and IntelliScripts can create medical reputations of individuals using data not covered by HIPAA or regulated by the Federal Trade Commission. These firms are also referred to as "reputational intermediaries". Acxiom started in 1969 as a small company with relatively little technology and the goal of amassing information on voters and consumers for direct marketing.[25] Today, Acxiom has detailed entries for more than 190 million people and 126 million U.S. households, including approximately 500 million active consumers worldwide.[26] The company's 23,000 servers, which are located in Little Rock, Arkansas collect and analyze more than 50 trillion data transactions per year.[27]

Natasha Singer of the New York Times is familiar with Acxiom's operations and stated in a 2012 interview, "If you are an American adult, the odds are that it knows things like your age, race, sex, weight, height, marital status, education level, politics, buying habits, household health worries, vacation dreams and more." Companies like Acxiom sells this wealth of information to anyone willing to bid the most for the information and use it to market specifically and directly to consumers. In 2011, Acxiom made a reported profit of $77.26 million.[28] IntelliScripts provides consumer's personal drug profiles to insurers. Insurers can use IntelliScripts to gather prescription information in real time and then review an online report.[29]

---

[25] What Is Acxiom Corp, And How Does It Know Your Mother's Maiden Name?, 2012 WLNR 13055499
[26] Id.
[27] Id.
[28] Id.
[29] http:// www.milliman.com/expertise/healthcare/products-tools/intelliscript

IntelliScripts says it sells prescription data to more than 75 health, life, and long-term-care insurance companies. Milliman, a large Seattle consulting firm, acquired the company in 2005.[30]

Neither IntelliScripts nor Acxiom are covered entities, therefore do not fall within the purview of HIPAA nor regulations promulgated to enforce HIPAA. The purpose of these firms is clearly marketing and not the provision of health care, thus it is uncontested that these entities do not constitute covered entities. According to HIPAA, Covered entities include health plans, health care clearinghouses and health care providers who transmit any health information in electronic form in connection with health care transactions covered by HIPAA.[31] The absence of rules and regulations gives firms like IntelliScripts and Acxiom practically free reign to accumulate troves of information and do with it what they please. All the while, consumers that may be offended at the thought of their personal information being dispersed may have no understanding of the secondary market for their health information; much less would any consumer have reason to believe massive profiles exist on nearly every American adult as mentioned above. The market created for pharmaceutical companies, by reputational intermediaries causes unfair surprise to consumers, an invasion of privacy of the American people and a lack of transparency in an inherently secretive industry.

VI. Current Regulatory Approach

a. Data Brokers

"Data brokers are companies that collect personal information about consumers from a variety of public and non-public sources and resell the information to other companies. In many ways, these data flows benefit consumers and the economy; for example, having this information about consumers enables companies to prevent fraud. Data brokers also provide data to enable

[30] http://www.businessweek.com/stories/2008-07-22/they-know-whats-in-your-medicine-cabinet
[31] 45 F.F.R. §§ 160.103

their customers to better market their products and services."[32] "Recent amendments to the FCRA have precluded states from enacting legislation that would offer more comprehensive privacy protections."[33] "The FCRA defines a consumer reporting agency and what activities are covered under its provisions. However, these provisions are written is such a way that data brokers are able to define themselves out of the FCRA's grasp."[34]

Logan Danielle Wayne authored a comment entitled, "The Data-Broker Threat: Proposing Federal Legislation to Protect Post-Expungement Privacy" and discussed why state statutes are inadequate to protect consumers from the potential abuses inherent in the data broker industry. "Because data brokers maintain and distribute records throughout the nation [state legislation] is inadequate." [35] While Wayne's comment focuses on data brokers in the criminal context, the same can be said for brokers that amass consumer's health information. Unless all 50 states enacted comprehensive legislation simultaneously, one (or even several) state's effort would be insufficient. Similarly, "the data brokers are not in privity of contract with users, therefore, users cannot sue them on a contract theory, and thus third-party entities have little incentive to protect, or even ensure the accuracy of, personal data," compiled in consumer profiles.[36] For those reasons, state law does not provide the consumer protection desired, and federal legislation focused on furthering consumer protection in the health context is ideal.

---

[32] FTC Website
[33] WestlawDoc1358 (*citing* Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. OF ILL. L. REV. 357, 380 (2006).)
[34] WESTLAW DOC
[35] WESTLAW DOC102 JCRLC 253
[36] WESTLAW DOC 18 COMLCON 155 (*citing* Marcy E. Peek, *Beyond Contract: Utilizing Restitution to Reach Shadow Offenders and Safeguard Information Privacy, in* SECURING PRIVACY IN THE INTERNET AGE 137 (Anu-pam Chander et al. eds., 2008).

b. FTC Approach

The Federal Trade Commission's attempts to close the gap in consumer protectionism include the federal Fair Credit Reporting Act ("FCRA"), which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. [37] The scope of the act includes agencies that sell information about medical records such as Acxiom and IntelliScripts.[38] According to the act, consumers must be notified if information in their file is used against them to deny an application for credit, employment, or insurance and must supply the consumer with the name, address and telephone number of the agency that provided the information.[39] Furthermore, the consumer may request any and all information contained in the files of a consumer reporting agency, and the request will be granted free of charge in certain circumstances.[40]

The statute seeks to address Paula and Walter Sherman's circumstances in which an individual's personal file is incomplete and/or inaccurate. In such cases, the individual is supposed to have the right to dispute the information and if successful the consumer-reporting agency must correct or delete the disputed content. [41] "If a consumer reporting agency, or, in some cases, a user of consumer reports or a furnisher of information to a consumer reporting agency violates the FCRA, you may be able to sue in state or federal court."[42] However, FCRA fails to provide individuals with information as to the extent of their profile that has been

[37] Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681 et seq.
[38] FCRA RIGHTS SUMMARY
[39] Id.
[40] Id.
[41] Id.
[42] Id.

distributed and to whom the profile has been released. This gap fails to protect one from 'downstream sale of his nonfinancial personal information.'"[43]

The FCRA aims to tackle the concerns of consumers worried about the accumulation and misuse of PHI, internet browsing history, purchase history, etc. Commercial data brokers, however, are not subject to the limitations of the FCRA, as they are not considered credit-reporting agencies. [44] Prior to the FCRA, insurance companies added boilerplate language in the fine print of their applications to comply with the privacy provisions of HIPAA. [45] With the implementation of FCRA, the FTC has merely required firms like IntelliScripts to tell insurers of the consumer rights discussed in the paragraph above so that the insurers could pass the appropriate information along to their customer beneficiaries.[46] What comfort does this provide to those being insured? The following discussion illustrates why the approach taken by the Federal Trade Commission via the Federal Credit Reporting Act is an inadequate protection of consumer privacy and does not protect the average consumer/patient from the unfair surprise and potential hardship that results as a consequence of their information being misused.

c. FTC v. IntelliSripts

On February 6, 2008 the Federal Trade Commission took action in hopes of initiating a shift towards greater consumer protection. The FTC filed a complaint against IntelliScripts (and parent corporation Milliman, Inc.) alleging that IntelliScripts violated the FCRA by keeping

[43] Sarah Ludington, Reigning in the Data Traders: A New Tort for the Misuse of Personal Information, 66 Md. L. Rev. 140, 146 (2006)
[44] Id.
[45] http://www.businessweek.com/stories/2008-07-22/they-know-whats-in-your-medicine-cabinet
[46] Id.

consumers from discovering the exchanges of consumer profiles that occurred between IntelliScripts and insurance company purchasers.[47]

Section 603(d) of the Fair Credit Reporting Act defines a consumer report.[48] In the FTC's complaint against IntelliScripts, the FTC claimed that the medical profile generated by IntelliScripts constituted a consumer report under the act because "it bears on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living, which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing a consumer's eligibility for credit or insurance." [49] As a result, the FTC then argued that IntelliScripts regularly furnished these reports to third parties in exchange for money by way of interstate commerce making it a "consumer reporting agency"[50] as defined in Section 603(f) of the FCRA.[51] Arguing that the profiles constituted consumer reports; therefore that IntelliScripts acted as a consumer-reporting agency, brought IntelliScripts' business model within the gambit of FTC enforcement of the FCRA.

> Section 607(d) of the Fair Credit Reporting Act, 15 U.S.C. § 1681e(d), requires that any consumer reporting agency provide, to any person to whom it provides a consumer report; a "Notice To Users of Consumer Reports: Obligations of Users Under the FCRA," the required content of which is set forth in 16 CFR 698, Appendix H. Respondent has failed and continues to fail to provide

---

[47] Complaint at 2, In the Matter of Milliman, Inc., (2007) (Case No. 062-3189)
[48] "Any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for: credit or insurance to be used primarily for personal, family, or household purposes. 15 U.S.C. §1681a(d)
[49] Complaint at 2, In the Matter of Milliman, Inc., (2007) (Case No. 062-3189)
[50] Section 603(f) 15 U.S.C. §1681a(f)
[51] Id.

> this notice to insurance companies that purchase medical profiles generated by IntelliScripts.[52]

IntelliScripts did not comply with the notice aforementioned notice requirement, and subsequently entered into the settlement agreement mentioned above. The FTC and IntelliScripts came to a settlement agreement[53] and, unfortunately, the Commission "merely required disclosure if prescription information causes denial of coverage or some other adverse action; the agency imposed no penalties."[54] Thus, consumers and the federal government are moving forward solely with the assurances from MedPoint and IntelliScripts that they are now complying with the Commission's instructions. There are no safeguards in place to assure that insurers are complying with the disclosure and notice requirements set forth by the settlement agreement and therefore no assurance that consumers being insured are being notified when the medical information gathered by reputational intermediaries and data brokers is influencing insurers decisions to accept or deny applicants.

d. FTC Investigation

On December 18, 2012, the Federal Trade Commission issued nine orders for information to analyze the data broker industry's collection and use of consumer data. The orders required the companies to provide the FTC with more comprehensive details about their practices including how they collect and use data about consumers that they compile. "The agency will use the information to study privacy practices in the data broker industry."[55] The investigation followed a report dispersed by the FTC earlier in the year that set guidelines for data brokerage companies to follow to achieve best practices, "based on the concepts of privacy

[52] Complaint at 2, In the Matter of Milliman, Inc., (2007) (Case No. 062-3189)
[53] Agreement Containing Consent Order, In the Matter of Milliman, Inc., (2007) (Case No. 062-3189)
[54] http://www.businessweek.com/stories/2008-07-22/they-know-whats-in-your-medicine-cabinet
[55] http://ftc.gov/opa/2012/12/databrokers.shtm

by design, consumer control, and increased transparency for the collection and use of consumer data."[56] The report coupled with the demand for information reflects some of the privacy concerns discussed above. "Consumers are often unaware of the existence of data brokers as well as the purposes for which they collect and use consumers' data. This lack of transparency also means that even when data brokers offer consumers the ability to access their data, or provide other tools, many consumers do not know how to exercise this right."[57]

Data brokerage firms and reputational intermediaries should closely monitor the FTC's recent focus on consumer protectionism. The agency's actions signify an intention to hold companies like IntelliScripts, Acxiom and the nine companies listed in the FTC order, accountable for their failures to maintain transparent practices while keeping consumers informed about the depth and content of profiles that exist containing their individual information. Specifically, "the FTC will use the responses it receives to prepare a study and to make recommendations on whether, and how, the data broker industry could improve its privacy practices."[58] While there are currently no laws directly on point to govern these issues, a federal regulatory framework is discussed below and the FTC commissioner will probably continue to put pressure on these companies to improve transparency and better business practices.

IV. PROPOSED REGULATION

In general, Congress has the power to regulate the channels of commerce and all things in, of or about interstate commerce.[59] The purchasing and/or sale of consumer profiles created

---

[56] Id.
[57] Id.
[58] Id.
[59] Original authority for commerce power is derived from Article I, Section Eight, Clause Three of the United States Constitution, which provides inter alia that Congress shall have the power to "regulate Commerce with foreign Nations, and among the several States." U.S. Const. art. I, §8, cl. 3. However, that power has been interpreted by the judiciary to include the power to regulate

by reputational intermediaries and data brokers across state lines are clearly part of interstate commerce. Thus, Congress has the constitutional authority to regulate the data broker industry under the Commerce Clause, and doing so would help create a uniform, clear and predictable regulatory scheme for consumers and health professionals alike.

a. Cover Reputational Intermediaries Under HIPAA

In the context of reputational intermediaries, one possible improvement to the current regulatory framework is to make reputational intermediaries covered entities under the Health Insurance Portability and Accountability Act. As the number of entities capable of accessing patient health information increases, the risk of security breaches, re-identification and risk of abuse of the privilege to collect and disseminate personal health information increases. An attempt to alleviate some of consumer's concerns in this context should include an expanded definition of "covered entities" under HIPAA. If HIPAA's definition of covered entities is broadened to include reputational intermediaries, the Department of Health and Human Services will have the authority as a regulatory body to tighten the free flow of patient health information (such as prescription history) by and from companies like IntelliScripts and Acxiom. Practically, the regulation listing the covered entities already in place under HIPAA[60] could add, "and any private entity that accumulates and/or disseminates PHI for the purpose of earning a profit". Practically speaking, that would probably provide very little change in the practices in place today. As mentioned above, there are numerous exceptions that allow covered entities to disclose PHI without disclosure to, or consent from, the patient-consumer.

---

the channels of interstate commerce, all things that fall within interstate commerce, and those things that substantially affect interstate commerce. See, e.g., Nat'l Labor Relations Bd. v. Jones & Laughlin Steel Corp., 301 U.S. 1 (1938); Champion v. Ames, 188 U.S. 321 (1903) (in, of, and about interstate commerce); Gibbons v. Ogden, 22 U.S. 1 (1824) (channels of interstate commerce).

[60] 45 C.F.R. §§ 160.103

To have a meaningful effect on the industry and the protection of patient's health information, the requirements for covered entities as well as the penalties for failure to comply with the regulations must also be revisited. For example, the proposed regulations should include an accounting of disclosures by covered entities. When an individual's PHI is disclosed or viewed by a party previously not privy to that information, an accounting of the disclosure should be made to the patient. Doing so will put the onus on the patient to monitor their own information, while adding mere administrative costs to the entities that are in possession of the PHI to begin with. Furthermore, if an entity in possession of an individual's information wishes to sell it to a data brokerage company, or other interested entity, they may do so only with the consent of the patient. This requirement will naturally: improve the transparency of the data brokerage/reputational intermediary industries; increase consumer knowledge of the personal profiles that have been accumulated over time and provide for greater individual control over those profiles. The consumer's knowledge of the care and how their records are being maintained should also be an aspect of that quality that Congress begins to pay more attention to.

b. IMS v. Sorrell

"When physicians prescribe medications to patients, pharmacies are under the duty to track certain prescriber-specific data by law. Unbeknownst to patients, and often to doctors themselves, the pharmacies sell this precious commodity to data mining companies that analyze and format the information for the pharmaceutical industry."[61] Data miners are usually responsible for analyzing the data for pharmaceutical companies so the pharmaceutical industry

[61] Isabelle Bibet-Kalinyak, A Critical Analysis of Sorrell v. Ims Health, Inc.: Pandora's Box at Best, 67 Food & Drug L.J. 191, 195 (2012).

can focus their marketing efforts and target patients and doctors based on the prescribing habits of physicians.[62]

Pharmacies sell "prescriber-identifying information to data miners, "who produce reports on prescriber behavior and lease their reports to pharmaceutical manufacturers." [63] Pharmaceutical companies then employ "detailers" to focus marketing efforts and increase sales based on the information discovered from the prescriber-identifying information.[64] Between 2006 and 2010, twenty-six states proposed legislation that would limit the use of PI data for commercial/marketing purposes.[65] In 2007, Vermont passed the Confidentiality of Prescription Information Act, which required among other things that records containing a doctor's prescribing practices not be sold or used for marketing purposes unless the doctor consented.[66] Specifically, the law provided:

> A health insurer, a self-insured employer, an electronic transmission intermediary, a pharmacy, or other similar entity shall not sell, license, or exchange for value regulated records containing prescriber-identifiable information, nor permit the use of regulated records containing prescriber-identifiable information

[62] Data mining is defined as "the process of discovering interesting patterns in databases that are useful in decision making." Indranil Bose & Radha K. Mahapatra, Business Data Mining - A Machine Learning Perspective, 39 Info. & Mgmt. 211, 211 (2001). Data miners are firms involved in the business of collecting, analyzing, and reselling that information. *Id.* The three data-mining companies who filed the initial lawsuit against Vermont, Maine, and New Hampshire are IMS Health, Inc., SDI (formerly Verispan LLC), and Source Healthcare Analytics Inc., a division of Wolters Kluwer Health, Inc. Brief for Respondents at 1 Sorrell v. IMS Health Inc., 131 S.Ct. 2653 (2011) (No. 10-779), 2011 WL 1149043 at 1. For a thorough review of pharmaceutical companies' use PI information and its effect on patients, see David Orentlicher, *Prescription Data Mining and the Protection of Patient's Interests*, 38 J.L. Med. & Ethics 74 (2010). Isabelle Bibet-Kalinyak, A Critical Analysis of Sorrell v. Ims Health, Inc.: Pandora's Box at Best, 67 Food & Drug L.J. 191, 241 (2012).

[63] Sorrell v. IMS Health Inc., 131 S. Ct. 2653, 2656 (2011)

[64] 67 Food & Drug L.J. 191, 195 (2012).

[65] Marcia M. Boumil et. al., Prescription Data Mining, Medical Privacy and the First Amendment: The U.S. Supreme Court in Sorrell v. Ims Health Inc., 21 Annals Health L. 447, 453 (2012).

[66] Act 80 § 4631(d) (Act 80).

> for marketing or promoting a prescription drug, unless the prescriber consents as provided in subsection (c) of this section. Pharmaceutical manufacturers and pharmaceutical marketers shall not use prescriber-identifiable information for marketing or promoting a prescription drug unless the prescriber consents as provided in subsection (c) of this section.[67]

Thus, the law "limited, but did not prohibit, the purchase and sale of PI data used to promote the marketing of prescription drugs. If the prescriber consented to the sale or use of the PI data, the restriction would not apply. Further, the law contained a number of exceptions to the restriction, including use for scientific research, compliance issues, pharmacy reimbursement, and other purposes provided by law."[68] Three Vermont data miners, IMS Health Inc., SDI and Source Healthcare Analytics Inc., and Pharmaceutical Research and Manufacturers of America, a national association of brand-name drug manufacturers contended that the Vermont statute above violated their freedom of speech under the First Amendment to the United States Constitution.[69] In response, Vermont argued "its prohibitions safeguard medical privacy and diminish the likelihood that marketing will lead to prescription decisions not in the best interests of parents or the State."[70] Essentially, Vermont attempted to combat the very issues discussed throughout this paper on their own. "Speech in aid of pharmaceutical marketing; however, is a form of expression protected by the Free Speech Clause of the First Amendment. As a consequence, Vermont's statute must be subject to heightened judicial scrutiny."[71] The First Amendment to the U. S. Constitution guarantees that Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the

---

[67] Id.
[68] Marcia M. Boumil et. al., Prescription Data Mining, Medical Privacy and the First Amendment: The U.S. Supreme Court in Sorrell v. Ims Health Inc., 21 Annals Health L. 447, 448 (2012).
[69] Sorrell, 131 S. Ct. 2653 (2011).
[70] Id.
[71] Id.

press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.[72] The United States District Court for the District of Vermont denied relief. However, the United States Court of Appeals for the Second Circuit reversed, holding that the law violated the First Amendment by restricting the speech of the companies without adequate justification. [73]

Justice Anthony Kennedy delivered the opinion of the Supreme Court, Joined by Chief Justice Roberts, Scalia, Thomas, Alito and Sotomayor.[74] The majority held that the law violated the First Amendment and affirmed the judgment of the Court of Appeals.[75] Firstly, the court found that the Vermont statute placed content and speaker based restrictions on speech. Although that finding was not per se fatal for the state statute, the result is that the statute could only succeed if it satisfied a heightened judicial scrutiny.[76] The majority rejected Vermont's contention that the law was a commercial regulation and not a regulation of speech on the grounds that the law imposed more than an incidental burden on speech.[77] Thus, the Court moved on to the analysis of whether the Vermont statute met the heightened judicial scrutiny. "To sustain the targeted, content-based burden the law imposes on protected expression, Vermont must show at least that the statute directly advances a substantial governmental interest, and that the measure is drawn to achieve that interest."[78] Vermont unsuccessfully argued that the

---

[72] U.S. CONST. Amend. I-Full Text
[73] Sorrell, 131 S.Ct. 2653 (2011).
[74] Id.
[75] Id.
[76] "Act 80 is designed to impose a specific, content-based burden on protected expression. It follows that heightened judicial scrutiny is warranted. *See* Cincinnati v. Discovery Network, Inc., 507 U.S. 410, 418 (1993) (applying heightened scrutiny to a "categorical prohibition on the use of news racks to disseminate commercial messages." Id. at 2664.
[77] Id. at 2668.
[78] Id. at 2657 (*Citing* Greater New Orleans Broadcasting Assn., Inc. v. United States, 527 U.S. 173, 184 (1999).

law was necessary to protect medical privacy, physician confidentiality and maintain the integrity of the doctor-patient relationship and to achieve improved public health care.[79] The Court reasoned that "the state seeks to achieve its policy objectives through the indirect means of restraining certain speech by certain speakers," which is an impermissible restriction under the First Amendment.[80] Vermont's statute attempted to stifle the use of particular information (prescriber-identifying information) for the purposes of being sold or used in connection with marketing (speech). However, the Court made a suggestion for future lawmakers stating, "if Vermont's statute provided that prescriber-identifying information could not be sold or disclosed except in narrow circumstances then the State might have a stronger position."[81]

Practically speaking, the Supreme Court's decision in Sorrell prohibits state statutes focused on data mining, data brokerage companies and reputational intermediaries alike. The court will likely find that such statutes discriminate against the content and speakers in these industries and should be held to be a violation of the First Amendment. Furthermore, the Court's decision will not be limited to prescriber-identifying information. The decision will likely govern all information disclosure because the court treated the information found in the patient profiles no different from any other type of commercial speech.

As a result, it is clear that similar state action is not a viable alternative for protecting the privacy of patient PHI. However, the Court clearly left a path for lawmakers to follow in order to narrowly tailor future legislation to the legitimate and compelling interests of the state and thereby overcome a heightened judicial scrutiny that these laws will certainly face in the future. The Sorrell majority did not address whether the government may limit or prohibit the disclosure

[79] Id. at 2668.
[80] Id. at 2671
[81] Id. at 2672

of data to purely protect personal privacy. The statute in Vermont allowed the Court to avoid this question because it only restricted the use of data for particular uses (involving marketing, increased sales, etc.). Similarly, the Court in Sorrell was troubled by the fact that the statute restricted the disclosure of prescriber information under certain circumstances (marketing) but maintained an exception for purposes of research and education. The inequality of restricting supported the Court's finding that the statute was a content-based and speaker-based restriction on commercial speech. Had the statute had no preference or care who was utilizing the speech and just restricted it all together, the statute may have had a better chance of survival. This decision strikes at the heart of the dichotomy between protecting consumers from potential abuses of their information privacy, and the desired benefits of a free-flowing line of communication between patients and health care professionals, as well as, health care professionals amongst one another. The Court's intimated open mind towards future legislation is another reason why a reformed federal regulatory framework is most likely the best solution for the current flaws in consumer privacy protection. It will prove to be wise to provide strict protection to consumer information at the outset until the technology improves and can be more properly governed. Erring on the side of protecting the industries that profit tremendously from the dissemination of such information will make it more difficult to legislate in the future. Technology in general is evolving by the second and the potential harms outweigh the potential benefits if the technology is not reined in early.

V. CONCLUSION

The computerization of health records and consumer data should have a positive influence on the health care industry. Doctors should have a higher quantity of health information in front of them when seeing a patient and the information should be much more

detailed because of the ability to accumulate and transmit that information from patient to physician, as well as, between physicians and specialists. However, technology and those that reap profits from the fast-paced technological advances are usually a step ahead of the law.

The privacy of medical records is currently regulated by the Health Information Portability and Accountability Act (HIPAA). While HIPAA does not provide a private right of action for patients, it imposes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Privacy Rule requires appropriate safeguards to protect the privacy of personal health information (PHI), and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections. However, the restrictions on PHI only apply to "covered entities". Data brokers, data miners and reputational intermediaries do not qualify as covered entities; therefore, they are not governed by the restrictions of HIPAA. Thus, the secondary market for patient's PHI has exploded in recent years. Often, patients have no knowledge that massive profiles of data have been acquired throughout their lifetime, and those profiles are often sold, disseminated and could be used to re-identify the patient based on the prescription history, internet browsing, grocery shopping and other consumer information that companies have accumulated.

In addition to HIPAA, the FTC has the authority to regulate under the Fair Credit Reporting Act (FCRA). According to the act, consumers must be notified if information in their file is used against them to deny an application for credit, employment, or insurance and must supply the consumer with the name, address and telephone number of the agency that provided

the information. Commercial data brokers, however, are not subject to the limitations of the FCRA, as they are not considered credit-reporting agencies. Therefore, the limited rights consumers have under the Fair Credit Reporting Act are virtually non-existent when dealing with the privacy issue presented by the secondary market causing concern for health professionals everywhere. The FTC has taken a greater interest in reigning in the industry in recent years. They have filed complaints against reputational intermediaries like IntelliScripts and recently demanded reports from 9 data brokerage firms in an attempt to increase transparency and consumer awareness.