No. 10-779

IN THE

Supreme Court of the United States

WILLIAM H. SORRELL,
Attorney General of Vermont, et al.,

Petitioners,

v.

IMS HEALTH INC., et al.,

Respondents.

ON WRIT OF CERTIORARI TO THE SUPREME COURT OF THE UNITED STATES

BRIEF OF AMICUS ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF PETITIONERS

CINDY COHN
Counsel of Record
LEE TIEN
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
(415) 436-9333
cindy@eff.org

Attorneys for Amicus Curiae Electronic Frontier Foundation

234937

COUNSEL PRESS
(800) 274-3321 • (800) 359-6859

TABLE OF CONTENTS

Page

TABLE OF CONTENTS. i

TABLE OF CITED AUTHORITIES iii

INTERESTS OF AMICUS CURIAE. 1

INTRODUCTION AND SUMMARY OF THE ARGUMENT 1

I. Patient privacy is a substantial state interest 3

II. Plaintiffs' data-mining practices threaten patient privacy and trust 8

A. Re-identification of de-identified data is a significant privacy threat 8

B. The PI data at issue in this case presents grave re-identification issues. 12

C. The risk of re-identification threatens patient trust in electronic exchange . . . 15

III. If accepted, the Court of Appeals' analysis would threaten the constitutionality of myriad privacy-protective statutes and privileges. 18

Table of Contents

Page

A. Federal health privacy law, like the Vermont statute, restricts the commercial disclosure of medical records. 19

B. The Court of Appeals' analysis threatens many other privacy laws. . . . 24

CONCLUSION 27

TABLE OF CITED AUTHORITIES

Page

Cases:

American Motors Corp. v. Huffstutler,
575 N.E.2d 116 (Ohio 1991). 26

Bartnicki v. Vopper,
532 U.S. 514 (2001) 5, 6, 24

City of Ontario v. Quon,
130 S. Ct. 2619 (2010) 1

Dep't of Justice v. Reporters Comm. for Freedom of Press,
489 U.S. 749 (1989) 5

Doe v. Bolton,
410 U.S. 179 (1973). 7

Doe v. Southeastern Penn. Transp. Auth.,
72 F.3d 1133 (3d Cir. 1995). 6

Dun & Bradstreet v. Greenmoss Builders,
472 U.S 749 (1985). 7

Eisenstadt v. Baird,
405 U.S. 438 (1972). 7

Expo Chem. Co. v. Brooks,
572 S.W.2d 8 (Tex. Civ. App. 1978) 26

Cited Authorities

Page

F.E.R. v. Valdez,
58 F.3d 1530 (10th Cir. 1995) 6

Florida Star v. B.J.F.,
491 U.S. 524 (1989). 5

Griswold v. Connecticut,
381 U.S. 479 (1965). 7

IMS Health v. Ayotte,
490 F. Supp. 2d 163 (D.N.H. 2007),
rev'd, 550 F.3d 42 (1st Cir. 2008). 12

IMS Health v. Sorrell,
631 F. Supp. 2d 434 (D. Vt. 2009). 12

IMS Health v. Sorrell,
__ F.3d ___, 2010 WL 4723183
(2d Cir. 2010) 3-4, 7, 12

National Aeronautics and Space Administration v. Nelson,
131 S. Ct. 746 (2011) 1

NCTA v. FCC,
555 F.3d 996 (D.C. Cir. 2009). . . . . *passim*

Norman-Bloodsaw v. Lawrence Berkeley Lab.,
135 F.3d 1260 (9th Cir. 1998) 6

Page

Northwestern Memorial Hospital v. Ashcroft,
362 F.3d 923 (7th Cir. 2004) 23

Planned Parenthood of Missouri v. Danforth,
428 U.S. 52 (1976). 7

Schaill v. Tippecanoe County Sch. Corp.,
864 F.2d 1309 (7th Cir. 1988) 6

Trammel v. United States,
445 U.S. 40 (1980) 7

Trans Union Corp. v. FTC,
267 F.3d 1138 (D.C. Cir. 2001) denying reh'g in
245 F.3d 809 (D.C. Cir. 2001) 21, 22, 25

Trans Union Corporation v. FTC,
245 F.3d 809 (D.C. Cir. 2001) 5

United States v. Aguilar,
515 U.S. 593 (1995). 4, 26

Rules & Statutes:

U.S. Const. amend. I 1, 3, 6

12 U.S.C. § 3401 25

12 U.S.C. § 3401(1) 25

Cited Authorities

	Page
12 U.S.C. § 3402	25
15 U.S.C. § 1681	25
15 U.S.C. § 6802(b)	25
18 U.S.C. § 2702	24
18 U.S.C. § 2710(b)	25
18 U.S.C. § 2721	25
42 U.S.C. § 1320d	3
42 U.S.C. § 1320d-7	20
42 U.S.C. § 17921	3
42 U.S.C. § 17931(a)	20
42 U.S.C. § 17934(a)	20
42 U.S.C. § 17936(a)(1)	20
42 U.S.C. § 17931	19
42 U.S.C. § 1320d-5	19
42 U.S.C. § 1320d-6	19

45 C.F.R § 160 19

45 C.F.R. § 160.203 20

45 C.F.R § 164 19

47 U.S.C. § 222(a)..... 21

47 U.S.C. § 222(c)(1)..... 21

47 U.S.C. § 551(c)(1) 24

Unif. Trade Secrets Act § 1, 14 U.L.A. 433 (1985) . 26

American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-05, 123 Stat. 115 (2009) 3

2007 Vt. Acts & Resolves, No. 80, § 1 4

Vt. Stat. Ann. Tit. 18, § 4631 (West 2010) 2, 4

Other Authorities:

S. Rep. No. 99-541, reprinted in 1986 U.S.C.C.A.N. 3555 24

Executive Order 13335, *Incentives for the Use of Health Information Technology and Establishing the Position of the National Health Information Technology Coordinator*, 69 Fed. Reg. 24,059 (Apr. 27, 2004)..... 15

TABLE OF CITED AUTHORITIES

Page

In re Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, 22 F.C.C.R. 6927 (2007) 5

Arvind Narayanan & Vitaly Shmatikov, "Myths and Fallacies of 'Personally Identifiable Information,'" 53 Comms. of the ACM 24 (2010) 10

Arvind Narayanan & Vitaly Shmatikov, "Robust De-Anonymization of Large Sparse Datasets." 29 Procs. of the 2008 IEEE Symp. on Security & Privacy 111 (2008) 10, 11

Arvind Narayanan, "About 33 Bits," 33 Bits of Entropy, http://www.33bits.org/about 10, 11

Arvind Narayanan, "Your Morning Commute Is Unique: On the Anonymity of Home/Work Location Pairs," 33 Bits of Entropy (May 13, 2009), http://33bits.org/2009/05/13/your-morning-commute-is-unique-on-the-anonymity-of-homework-location-pairs/..... 11

Bradley Malin, "Re-Identification of Familial Database Records," Procs. of the 2006 Am. Med. Informatics Ass'n Annual Symp. 524 (2006) 12

TABLE OF CITED AUTHORITIES

Page

Cong. Research Serv., R40537, American Recovery and Reinvestment Act of 2009 (P.L. 111-5): Summary and Legislative History 34 (2009) . . . 19

Consumers and Health Information Technology: A National Survey, California HealthCare Foundation (Apr. 2010), http://www.chcf.org/publications/2010/04/consumers-and-health-information-technology-a-national-survey 16

David Blumenthal and Georgina Verdugo. *Statement on Privacy and Security, Building Trust in Health Info. Exchange*, U.S. Dep't of Health and Human Services (Jul. 8, 2010), available at http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__privacy_and_security/1147 . 17

David Blumenthal, "Effects of Market Reforms on Doctors and Their Patients," 15 Health Affairs 170 (May 1996) 17

Elizabeth Dugan *et al.*, "Development of Abbreviated Measures to Assess Patient Trust in a Physician, a Health Insurer, and the Medical Profession." 5 BMC Health Services Res. 64 (Oct. 2005) 17

From the Field: Sharing Experience and Findings from AHRQ-Funded Projects, Agency for Healthcare Research and Quality, http://healthit.ahrq.gov/portal/server.pt/community/ahrq_national_resource_center_for_health_it/650 (last modified Nov. 2010) 16

TABLE OF CITED AUTHORITIES

Page

Grigorios Loukides *et al.*, "Anonymization of Electronic Medical Records for Validating Genome-Wide Association Studies," 107 Procs. of the Nat'l Acad. of Sci. 7898 (2010). 11-12

Grigorios Loukides *et al.*, "The Disclosure of Diagnosis Codes Can Breach Research Participants' Privacy," 17 J. Am. Med. Informatics Ass'n 322 (2010). . . . 12

Health Information Security and Privacy Collaboration (HISPC), www.rti.org/hispc 16

Huey Jen Chen, *Trust and Health Service Use.* Florida Agency for Health Care Admin., 43 (May 2004), available at http://home.fmhi.usf.edu/common/file/ahca/ahca2004/2004-Chen.pdf. 17

Julia Angwin and Steve Stecklow, "'Scrapers' Dig Deep for Data on Web," WSJ.com (Oct. 12, 2010), http://online.wsj.com/article/SB10001424052748703358504575544381288117888.html . . . 15

Linda Dimitropoulos, *Privacy and Security Solutions for Interoperable Health Information Exchange: Impact Analysis* 4-7, 4-40 (2007), available at http://www.rti.org/pubs/phase2_impactanaly.pdf. 16

TABLE OF CITED AUTHORITIES

Page

Matthew Arnold, *For Pharmas, Online Video, Ad Exchanges are the Future (For Everybody Else, They're the Present)*, Medical Marketing & Media (May 25, 2010), http://www.mmm-online.com/for-pharmas-online-video-ad-exchanges-are-the-future-for-everybody-else-theyre-the-present/article/170984/. 14

Milt Freudenheim, "And You Thought a Prescription Was Private," N.Y. Times, Aug. 8, 2009 . . . . . 2, 9

New Way RA, http://www.newwayra.com 15

Paul Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization," 57 UCLA L. Rev. 1701 (2010) . . 10

Ralph Reubner & Leslie Ann Reis, "Hippocrates to HIPAA: A Foundation for a Federal Physician-Patient Privilege," 77 TEMP. L. REV. 505 (2004) 6

President's Council of Advisors on Science and Technology, *Realizing the Full Potential of Healthcare Technology to Improve Healthcare for Americans* 46 (Dec. 2010), available at http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-health-it-report.pdf. 18

INTERESTS OF AMICUS CURIAE[1]

The Electronic Frontier Foundation ("EFF") is a nonprofit, member-supported civil liberties organization working to protect rights in the information society. EFF actively encourages and challenges government and the courts to support privacy and safeguard individual autonomy. As part of its mission, EFF has often served as counsel or amicus in privacy cases, such as *National Aeronautics and Space Administration v. Nelson*, 131 S.Ct. 746 (2011), and *City of Ontario v. Quon*, 130 S. Ct. 2619 (2010).

INTRODUCTION AND SUMMARY OF THE ARGUMENT

This case presents no novel First Amendment issues. Instead, the Court of Appeals misunderstood the legal background of this case in a critical aspect: it wrongly asserted that the medical records at issue here are public. This error led the Court of Appeals to ignore the privacy interests at stake. Amicus therefore focuses on how the Vermont law at issue here protects patient privacy and how upholding the decision below could jeopardize much federal privacy law.

---

1. This brief is filed with the written consent of all parties. Consent letters are on file with the Clerk of the Court. No counsel for a party authored this brief in whole or in part, and no person or entity other than the amicus made a monetary contribution to the preparation or submission of this brief.

Vermont's Prescription Confidentiality Law, codified at Vt. Stat. Ann. Tit. 18, § 4631 (West 2010), prohibits regulated entities such as pharmacies from selling or using prescriber-identifiable (PI) medical records for marketing purposes without consent of the prescribing doctor. These PI records generally include at least the identity of the pharmacy, the name of the patient, information identifying the prescriber, the name, dosage, and quantity of the prescribed drug, and the date the prescription was filled, as well as the patient's age (or date of birth) and gender. In their original form, PI records reveal much sensitive personal information and unquestionably implicate important personal privacy interests.

Pharmacies sell PI records in "de-identified" form to the data-mining plaintiffs, who then manipulate the data and index it by proprietary patient ID tracking numbers for sale to customers such as the drug companies that are members of plaintiff PhRMA. As amicus discusses below, however, there are substantial concerns today about the efficacy of this "de-identification" for protecting privacy given the enormous trade in consumer data. Such data mining of PI records exposes patients' prescription histories and thus their underlying medical conditions, allowing companies to match prescriptions with specific patients.[2]

Vermont's law thus protects patient privacy by requiring express consent from physicians before pharmacies may disclose their patients' PI records, an utterly unremarkable purpose given societal recognition

2. Milt Freudenheim, *And You Thought a Prescription Was Private*, N.Y. Times, Aug. 8, 2009, at BU1.

of the doctor-patient privilege and doctors' ethical duties of confidentiality to their patients.

Many federal statutes similarly restrict the flow of confidential data for commercial purposes based on consent. Indeed, the primary federal health privacy law—the Health Insurance Portability and Accountability Act (HIPAA), 42 U.S.C. § 1320d *et seq.* (2010)[3]—not only restricts disclosure of patient records for marketing purposes, but also authorizes the states to protect patient privacy more stringently.[4] To uphold the Court of Appeals here could cast grave doubts about the constitutionality of all such laws—some of which have already been found permissible under the First Amendment. In short, Vermont's Prescription Confidentiality Law protects patients against unwanted invasions of privacy in a way that is fully consistent with the First Amendment as well as federal privacy law and policy.

I. Patient privacy is a substantial state interest.

The Court of Appeals apparently believed that PI records did not implicate patient privacy, saying that "the concern that patient information can be gleaned from PI data is not reduced in any way by section 17, and the statute does not prohibit wide public dissemination of PI data." *IMS Health v. Sorrell*, ___ F.3d ___(2d Cir. 2010),

3. HIPAA was significantly amended by the Health Information Technology for Economic and Clinical Health Act (HITECH Act), codified at 42 U.S.C. § 17921 *et seq.* (2010), as part of the American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-05, 123 Stat. 115 (2009).

4. See discussion *infra* at n. 15 and accompanying text.

2010 WL 4723183, *10. The court thus concluded that Vermont's interest in medical privacy was too speculative to be considered. *Ibid.*

Remarkably, the Court of Appeals seemed to focus only on the challenged statute and ignored the background framework of patient privacy. Pet'r's Br. 5-6 (explaining how both Vermont law and federal health privacy law obligate pharmacies to maintain privacy and confidentiality of prescription records). This legal error alone warrants reversal. *See United States v. Aguilar*, 515 U.S. 593, 605 (1995) ("As to one who voluntarily assumed a duty of confidentiality, governmental restrictions on disclosure are not subject to the same stringent standards that would apply to efforts to impose restrictions on unwilling members of the public.") (citation omitted).

Correctly understood, the Vermont law clearly intends to protect medical privacy:

> "Health care professionals in Vermont who write prescriptions for their patients have a reasonable expectation that the information in that prescription, including their own identity and that of the patient, will not be used for purposes other than the filling and processing of the payment for that prescription. Prescribers and patients do not consent to the trade of that information to third parties, and no such trade should take place without their consent."

2007 Vt. Acts & Resolves, No. 80, § 1(29), codified at Vt. Stat. Ann. Tit. 18, § 4631 (West 2010).

This Court recognizes that privacy is at least a

substantial government interest. *Bartnicki v. Vopper*, 532 U.S. 514, 518 (2001) (characterizing "the interest in individual privacy" as one "of the highest order."); *Florida Star v. B.J.F.*, 491 U.S. 524, 533 (1989) ("[P]rivacy rights are . . . plainly rooted in the traditions and significant concerns of our society.") (citation and internal quotation marks omitted); *Dep't of Justice v. Reporters Comm. for Freedom of Press*, 489 U.S. 749, 763 (1989) ("[B]oth the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person.").

So do the courts of appeal. *See, e.g.*, *NCTA v. FCC*, 555 F.3d 996, 1000 (D.C. Cir. 2009) ("the government has a substantial interest in protecting the privacy of customer information") (upholding, under the commercial speech doctrine, agency order requiring opt-in consent for telecommunications carriers' use of customer information for third-party marketing purposes)[5]; *Trans Union Corporation v. FTC*, 245 F.3d 809, 818 (D.C. Cir. 2001) ("[W]e have no doubt that this interest—protecting the privacy of consumer credit information—is substantial.") (upholding, under the commercial speech doctrine, agency implementation of the Fair Credit Reporting Act).

Where medical privacy is concerned, societal recognition is at least as great. HIPAA broadly protects the privacy of patient information. Most states, including

5. The order cited in NCTA, 555 F.3d at 1000, was *In re Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, 22 F.C.C.R. 6927 (2007).

Vermont, recognize the doctor-patient privilege.[6] And while federal evidence law does not recognize the doctor-patient privilege, some federal courts recognize an individual's right to confidentiality of medical records and medical communications, noting that "few subject areas [are] more personal and more likely to implicate privacy interests than that of one's health," *Norman-Bloodsaw v. Lawrence Berkeley Lab.*, 135 F.3d 1260, 1269 (9th Cir. 1998), and that medical information is "precisely the sort [of information] intended to be protected by penumbras of privacy," *Doe v. Southeastern Penn. Transp. Auth.*, 72 F.3d 1133, 1138 (3d Cir. 1995) (citation omitted); *see also F.E.R. v. Valdez*, 58 F.3d 1530, 1535 (10th Cir. 1995) (plaintiffs had a legitimate expectation of privacy in medical records); *Schaill v. Tippecanoe County Sch. Corp.*, 864 F.2d 1309, 1322 n.19 (7th Cir. 1988) (recognizing a substantial privacy interest in confidential medical information).

Furthermore, this medical privacy interest is simultaneously a highly protected speech interest—an interest in private speech. Privacy laws often restrict disclosure of personal information precisely in order to facilitate private communication. *Bartnicki*, 532 U.S. at 518 (characterizing "the interest … in fostering private speech" as one "of the highest order."); *id.* at 537 (Breyer & O'Connor, JJ, concurring) ("assurance of privacy helps to overcome our natural reluctance to discuss private matters when we fear that our private conversations may

6. *See* Ralph Reubner & Leslie Ann Reis, *Hippocrates to HIPAA: A Foundation for a Federal Physician-Patient Privilege*, 77 Temp. L. Rev. 505, 508, 564 n.439 (2004) (listing state doctor-patient privilege statutes).

become public…. the statutory restrictions consequently encourage conversations that otherwise might not take place."). Medical confidentiality helps ensure that patients will speak freely to their doctors about sensitive, personal matters. *Trammel v. United States*, 445 U.S. 40, 51 (1980) ("The privilege[] between . . . physician and patient limit[s] protection to private communications [and is] rooted in the imperative need for confidence and trust.").[7]

Admittedly, the Vermont law focuses on physician consent rather than patient consent. But this is no reason to ignore the patient's privacy. The doctor-patient relationship is close enough that doctors may in some cases assert the rights of their patients. *Planned Parenthood of Missouri v. Danforth*, 428 U.S. 52, 62 (1976); *Doe v. Bolton*, 410 U.S. 179, 188 (1973); *Eisenstadt v. Baird*, 405 U.S. 438, 445-446 (1972); *Griswold v. Connecticut*, 381 U.S. 479, 480-82 (1965). While direct patient consent would be preferable, Vermont may legitimately expect that doctors will act on behalf of their patients' privacy. Accordingly, the Vermont law is supported by a substantial government interest in medical privacy.

---

7. In contrast, the plaintiffs and the non-party pharmacies have a lesser speech interest because their exchange of PI medical data is "solely in the individual interest of the speaker and its specific business audience." *Dun & Bradstreet v. Greenmoss Builders,* 472 U.S 749, 762 (1985) (citation omitted); *Sorrell*, 2010 WL 4723183, at *22 ("[D]ata mining appellants actually *prohibit* their customers from disclosing the data they license to *anyone* else, much less the general public.") (emphases in original) (Livingston, J., dissenting).

II. Plaintiffs' data-mining practices threaten patient privacy and trust.

In rejecting Vermont's interest in medical privacy as "speculative," the Court of Appeals failed to appreciate how plaintiffs' data-mining practices threaten both patient privacy and patient trust in medical confidentiality. Changes in technology and in the overall information environment mean that traditional privacy safeguards such as de-identification are no longer reliable.

This does not mean that every patient can be identified today, of course. It does mean, however, that the risk exists and is growing with the increased volume and velocity of information exchange. The Vermont law thus furthers patient privacy and trust in medical confidentiality by allowing doctors to prevent PI data—their patients' confidential prescription records—from being shared for marketing purposes.

A. Re-identification of de-identified data is a significant privacy threat.

> More than 10 years after she tried without success to have a baby, Marcy Campbell Krinsk is still receiving painful reminders in her mail. The ads and promotions started after she bought fertility drugs at a pharmacy in San Diego.
>
> Marketers got hold of her name, and she found coupons and samples in her mail that shadowed the growth of an imaginary child — at first, for Pampers and baby formula, then for discounts

> on family photos, and all the way through the years to gifts suitable for an elementary school graduate.
>
> "I had three different in vitro procedures," said Ms. Krinsk, now 55, a former telecommunications executive who lives with her husband in San Diego. "To just go to the mailbox and get that stuff, time after time after time, it was just awful."
>
> Like many other people, Ms. Krinsk thought that her prescription information was private. But in fact, prescriptions, and all the information on them — including not only the name and dosage of the drug and the name and address of the doctor, but also the patient's address and Social Security number — are a commodity bought and sold in a murky marketplace, often without the patients' knowledge or permission.

Freudenheim, *supra* note 2.

Ms. Krinsk's story makes clear that widespread commerce in patient records poses significant risks to patient privacy. It is no longer true that the use and disclosure of de-identified patient health information raises little privacy risk to patients.

In the past few years, researchers Arvind Narayanan and Vitaly Shmatikov have revolutionized the field of re-identification. Based on their statistical research and techniques for re-identifying purportedly anonymous datasets, they conclude that "[t]he emergence of powerful re-identification algorithms demonstrates not just a flaw in

a specific anonymization technique(s), but the fundamental inadequacy of the entire privacy protection paradigm based on 'de-identifying' the data." Arvind Narayanan & Vitaly Shmatikov, *Myths and Fallacies of "Personally Identifiable Information*," 53 Comms. of the ACM 24, 26 (2010); *see* Arvind Narayanan & Vitaly Shmatikov, *Robust De-Anonymization of Large Sparse Datasets*. 29 Procs. of the 2008 IEEE Symp. on Security & Privacy 111 (2008); *see also* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701, 1704 (2010).

While the mathematics is complex, there are two basic reasons why re-identification is much easier today. First, computing resources are extremely large relative to population: "a lot of traditional thinking about anonymous data relied on the fact that you can hide in a crowd that's too big to search through. That notion completely breaks down given today's computing power: as long as the bad guy has enough information about his target, he can simply examine every possible entry in the database and select the best match." Arvind Narayanan, *About 33 Bits,* 33 Bits of Entropy, http://www.33bits.org/about (last visited Feb. 26, 2011).

The phrase "33 bits" makes a crucial point about re-identification. Knowing a person's gender, for instance, eliminates about half the population and is therefore worth about one bit. Given the current world population of roughly 6.6 billion people, only 33 independent bits of information are needed to uniquely identify an individual. *Ibid.*[8] And "33 bits is not really a lot. If your hometown

8. Thirty-three is the number of times 6.6 billion can be divided by 2 repeatedly, until the answer is 1 or less, or written mathematically, $\log_2(6600000000)$.

has 100,000 people, then knowing your hometown gives me 16 bits of entropy about you, and only 17 bits remain." *Ibid*. Location information like zip code is therefore extremely valuable for re-identification. *See generally* Arvind Narayanan, *Your Morning Commute Is Unique: On the Anonymity of Home/Work Location Pairs*, 33 Bits of Entropy (May 13, 2009), http://33bits.org/2009/05/13/your-morning-commute-is-unique-on-the-anonymity-of-homework-location-pairs/.

Second, many kinds of data can be used to help re-identify de-identified data, and such data is increasingly available in convenient, electronic form. Obviously, public or commercially available records that directly identify persons can serve as Rosetta Stones for re-identification. Fundamentally, however, any information that distinguishes one person from another can be used for re-identification.

"High-dimensional" data—data with many possible values—is especially useful because it reduces the likelihood that individuals are similar. *See generally* Narayanan & Shmatikov, *Robust De-Anonymization*, at 1. For instance, imagine an individual's prescription record as containing a column for each possible prescription medication, with cells or boxes checked for each medication he or she actually purchases. Such information has high dimensionality because the set of possible medications is large. A total prescription history that includes purchase dates is highly likely to be unique.

Unsurprisingly, considerable research in the medical arena now focuses on the re-identification threat. *See, e.g.*, Grigorios Loukides et al., *Anonymization of*

Electronic Medical Records for Validating Genome-Wide Association Studies, 107 Procs. of the Nat'l Acad. of Sci. 7898, 7902-03 (2010); Grigorios Loukides et al., *The Disclosure of Diagnosis Codes Can Breach Research Participants' Privacy*, 17 J. Am. Med. Informatics Ass'n 322, 322-23 (2010); Bradley Malin, *Re-Identification of Familial Database Records*, Procs. of the 2006 Am. Med. Informatics Ass'n Annual Symp. 524, 528 (2006) (using online sources like newspaper obituaries and death records to link de-identified family relations to named people).

B. The PI data at issue in this case presents grave re-identification issues.

The essential ingredients for re-identification today are the presence of a large, de-identified dataset to use in combination with other data. The PI data at issue here provides a rich dataset from which to start, as such records generally include at least the identity of the pharmacy, "the name of the patient, information identifying the prescriber, the name, dosage, and quantity of the prescribed drug, and the date the prescription was filled,"[9] as well as the patient's age (or date of birth)[10] and gender.[11]

---

9. *IMS Health v. Ayotte*, 490 F. Supp. 2d 163, 165 (D.N.H. 2007), *rev'd*, 550 F.3d 42 (1st Cir. 2008).

10. The record suggests that date of birth is normally transmitted. J.A. 248 ("If patients are over a certain age we have to de-identify their date of birth.") (testimony of Scott Tierney, CVS Caremark).

11. *IMS Health v. Sorrell*, 631 F. Supp. 2d 434, 441 (D. Vt. 2009), *rev'd, IMS Health v. Sorrell*, __ F.3d ___, 2010 WL 4723183 (2d Cir. Nov. 23, 2010).

Moreover, the "de-identified" data is organized via a persistent, unique patient ID number that allows data miners and their customers to track patients. Patient location information can be inferred from both prescriber and pharmacy location. As plaintiff Verispan explained:

> Q. All right. Can you just briefly explain this notion of the longitudinal data and how it is in particular that that information can be useful to pharmaceutical companies in marketing?
>
> A. So, we talked about the four P's a little bit earlier. We talked about the product, the prescriber, the payer and the pharmacy. We like to think that we do add the dimension of the fifth P, which is the Didentified [sic] patient, and what we do is as I alluded before we strip off all the HIPAA offending information and receive a linking code that would be able to determine a specific entity was traveling throughout our data base.
>
> Q. By identity, we mean Mark Ash has traveled from Vermont to California and back to North Carolina and I get prescriptions, am I the entity you're referring to?
>
> A. Yes. The person would be the entity that I'm referring to, and that person would get the code, I'm not going to rattle of 39 digits, let's just say it's code 12345, and every time that entity or individual came into our data set, that person would get the same linking code, which means that we don't know who that person is,

> but our ability to track that person over time and determine behaviors is intact and retained.
>
> Q. And can we connect that person, that unidentifiable person, 12345, with particular prescribers who write prescriptions for patient 12345?
>
> A. So, the common way that the data is used is to really link up any of the five P's together at the end of the day, and so if you're using the patient entity and you're linking that to the prescriber, that's one potential use of the data.

J.A. 161 (testimony of Jody Fisher, Verispan).

Such data can obviously be joined with traditional data sources such as public records, including hospital discharge databases, as well as transactional and demographic information from commercial databases. Pharmaceutical marketers are already "beginning to incorporate insurance claims data to identify patient populations."[12]

What has become increasingly evident, however, is that other rich data sources are available to industry. Websites where pharmaceutical companies request patients' age, zip code and other details could be used to

12. Matthew Arnold, *For Pharmas, Online Video, Ad Exchanges are the Future (For Everybody Else, They're the Present)*, Medical Marketing & Media (May 25, 2010), http://www.mmm-online.com/for-pharmas-online-video-ad-exchanges-are-the-future-for-everybody-else-theyre-the-present/article/170984/.

re-identify PI data. A rheumatoid arthritis site belonging to Centocor Ortho Biotech requests patient zip code and name. New Way RA, http://www.newwayra.com (last visited Feb. 27, 2011).[13] Social media sites where patients share information with each other are being "scraped" for data that could be used for re-identification. *See, e.g.*, Julia Angwin and Steve Stecklow, *'Scrapers' Dig Deep for Data on Web*, WSJ.com (Oct. 12, 2010), http://online.wsj.com/article/SB10001424052748703358504575544381288117888.html. There is every reason to believe that these risks will only increase over time.

C. The risk of re-identification threatens patient trust in electronic exchange.

Since 2004, it has been U.S. policy to encourage health care technology adoption. Exec. Order 13335, *Incentives for the Use of Health Information Technology and Establishing the Position of the National Health Information Technology Coordinator*, 69 Fed. Reg. 24,059 (Apr. 27, 2004).

Patients, however, are nervous about this shift from paper to electronic formats, and are most concerned about increased sharing of their health information, even if that sharing is for their benefit. A recent study found that 42 percent of those surveyed were uncomfortable with electronic health record sharing even if name, date of birth, address, and Social Security Number would not

13. Shareyourpain.com is a similar effort developed for Cephalon, a global pharmaceutical company. Shareyourpain.com requests ZIP, date of birth, name, and other information for site registrants who want to discuss cancer issues.

be shared and another 25 percent were not sure, while 15 percent who knew their information would be shared would hide information from their doctor and another 33 percent would consider hiding information. *Consumers and Health Information Technology: A National Survey*, California HealthCare Foundation 24-25 (Apr. 2010), http://www.chcf.org/publications/2010/04/consumers-and-health-information-technology-a-national-survey.

The Department of Health and Human Services (DHHS), through the Agency for Healthcare Research and Quality (AHRQ) and the Office of the National Coordinator for Health Information Technology, has similarly found[14] that patient trust in electronic health care exchanges is a core, vital component in technology adoption, and that health information exchange programs may suffer from a lack of patient and even provider adoption without patient trust. *See, e.g.*, Linda Dimitropoulos, *Privacy and Security Solutions for Interoperable Health Information Exchange: Impact Analysis* 4-7, 4-40 (2007), *available at* http://www.rti.org/pubs/phase2_impactanaly.pdf.

---

14. *The Health Information Security and Privacy Collaboration*, RTI International, www.rti.org/hispc (last visited Feb. 26, 2011). This DHHS project had the goal of developing and testing solutions for the privacy and security of national and state health information exchange. The series of multi-year studies and reports is available at *From the Field: Sharing Experience and Findings from AHRQ-Funded Projects*, Agency for Healthcare Research and Quality, http://healthit.ahrq.gov/portal/server.pt/community/ahrq_national_resource_center_for_health_it/650 (last modified Nov. 2010), and at Health Information Security and Privacy Collaboration (HISPC), www.rti.org/hispc (last visited Feb. 26, 2011).

The importance of patient trust to health care and therapeutic relationships is hardly new, given our social recognition of doctor-patient confidentiality. Without patient trust in various health care settings and situations, patients may not utilize health services. *See* David Blumenthal, *Effects of Market Reforms on Doctors and Their Patients*, 15 Health Affairs 170, 184 (May 1996); *see also* Elizabeth Dugan et al., *Development of Abbreviated Measures to Assess Patient Trust in a Physician, a Health Insurer, and the Medical Profession*. 5 BMC Health Services Res. 64, 68 (Oct. 2005); Huey Jen Chen, *Trust and Health Service Use.* Florida Agency for Health Care Admin., 43 (May 2004), *available at* http://home.fmhi.usf.edu/common/file/ahca/ahca2004/2004-Chen.pdf.

Unsurprisingly, federal policymakers consistently emphasize that engendering patient trust is a core value for modern health information technology and exchanges. David Blumenthal and Georgina Verdugo. *Statement on Privacy and Security*, Building Trust in Health Info. Exchange, U.S. Dep't of Health and Human Services (Jul. 8, 2010), *available at* http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__privacy_and_security/1147 (follow "Read Joint OCR-ONC Statement" hyperlink) ("[O]ne of the Department's guiding principles is that the benefits of health IT can only be fully realized if patients and providers are confident that electronic health information is kept private and secure.").

More recently, the President's Council of Advisors on Science and Technology recommended:

> To build and maintain the public's trust in health IT requires comprehensive privacy and

> security protections that are based on fair information practices and set clear rules on how patient data can be accessed, used and disclosed, and that are adequately enforced. An individual's right to have some meaningful choice in how their information is shared is one important component of a comprehensive set of protections. Where such choices are provided, either in law or by policy, they must be persistently honored.

PCAST, Report to the President, *Realizing the Full Potential of Healthcare Technology to Improve Healthcare for Americans* 46 (Dec. 2010), *available at* http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-health-it-report.pdf.

Currently, neither patients nor doctors have a choice about the dissemination of "de-identified" PI data. Such choice must exist for patients and providers to trust information to flow freely through health information exchanges. The Vermont statute appropriately allows for such choice in today's computing and data environment.

III. If accepted, the Court of Appeals' analysis would threaten the constitutionality of myriad privacy-protective statutes and privileges

Amicus agrees with Vermont's argument that the Prescription Confidentiality Law survives intermediate scrutiny under the commercial speech doctrine. Amicus therefore focuses on the grave implications of upholding the Court of Appeals' decision that the Vermont law is unconstitutional: many federal privacy laws might also be

unconstitutional, immunizing the wholesale disclosure of sensitive private information by businesses. In short, the Court of Appeals' analysis proves far too much.

A. Federal health privacy law, like the Vermont statute, restricts the commercial disclosure of medical records.

Federal health privacy law is the most obvious example. Under the HIPAA Privacy Rule, 45 C.F.R §§ 160, 164 (2010), disclosure of individually identifiable health information by entities covered by HIPAA is generally regulated. *See, e.g.*, 42 U.S.C. §§ 1320d-5, 1320d-6 (imposing fines and criminal punishments for the knowing disclosure of "individually identifiable health information to another person.").

Congress recently buttressed these basic HIPAA protections in enacting new privacy provisions as part of the Health Information Technology for Economic and Clinical Health (HITECH) Act, 42 U.S.C. § 17931 *et seq.* (2009). *See generally* Cong. Research Serv., R40537, *American Recovery and Reinvestment Act of 2009 (P.L. 111-5): Summary and Legislative History* 34 (2009) ("Among other things, [the HITECH Act] establishes a breach notification requirement for health information that is not encrypted, strengthens enforcement of the HIPAA standards, and creates transparency by allowing patients to request an audit trail showing all disclosures of their electronic health information.").

Two sections of the HITECH Act are particularly relevant here. First, Congress strengthened consent requirements as to the sale of patient data for third-party

marketing purposes. 42 U.S.C. § 17936(a)(1). Second, Congress extended HIPAA's security and privacy rules to business associates of covered entities, and required that these obligations be incorporated into business associate agreements. *Id.* §§ 17931(a), 17934(a).

The point is simple: federal health privacy law clearly restricts the disclosure of patient records for commercial purposes in order to protect patient privacy. The Vermont law does the same thing.

Moreover, the federal government has made clear that the states may legislate to enhance federal privacy protections; HIPAA's "anti-preemption" provision authorizes Vermont to enact laws that expand the scope of medical record privacy.[15] Vermont's Prescription Confidentiality Law merely creates an additional state-law category of health information—PI data—under that protective umbrella.

A structurally analogous situation was presented in *NCTA v. FCC*, 555 F.3d 996 (D.C. Cir. 2009), where

15. 42 U.S.C. § 1320d-7 ("A regulation promulgated under paragraph (1) shall not supersede a contrary provision of State law, if the provision of State law imposes requirements, standards, or implementation specifications that are more stringent than the requirements, standards, or implementation specifications imposed under the regulation."). The HIPAA Privacy Rule makes clear that it is intended as a "federal floor" for privacy protection, allowing state law to control where a "provision of State law relates to the privacy of individually identifiable health information and is more stringent than a standard, requirement, or implementation specification adopted under [the Privacy Rule]." 45 C.F.R. § 160.203.

telephone service providers brought a First Amendment challenge to FCC telephone privacy rules under which carriers could not share customer information for third-party marketing purposes without opt-in customer consent. *See* n. 5, *supra*.

Like the Vermont law here, the FCC's order was adopted pursuant to Congressional policy that generally protects customer privacy. 47 U.S.C. § 222(a) (2010) (imposing on carriers "duty to protect the confidentiality of proprietary information of . . . consumers."); *id.* § 222(c)(1) (prohibiting carriers from otherwise using, disclosing or allowing access to such information except "as required by law" or "with the approval of the customer.").

The D.C. Circuit squarely rejected the providers' First Amendment challenge using reasoning that is fully applicable here. The court recognized that the providers were not challenging the underlying federal statute, thereby conceding at least two crucial points: "that the government has a substantial interest in protecting the privacy of customer information and that requiring customer approval advances that interest." *NCTA*, 555 F.3d at 1000.

The court then asked whether the opt-in consent provision directly advanced this interest. "Here again petitioners' agreement that § 222 complies with the First Amendment all but settles the issue. The privacy of customer information cannot be preserved unless there are restrictions on the carrier's disclosure of it." *Id.* at 1001 (citing *Trans Union Corp. v. FTC*, 267 F.3d 1138, 1142 (D.C. Cir. 2001)) ("The government cannot promote its interest (protection of personal financial data)

except by regulating speech because the speech itself (dissemination of financial data) causes the very harm the government seeks to prevent.") (upholding similar regime requiring opt-in consent for the sharing of customer credit information), *denying reh'g in* 245 F.3d 809 (D.C. Cir. 2001).

Indeed, the two cases feature strikingly similar arguments. In *NCTA*, the carriers argued that there was no evidence that the joint venturers or independent contractors who receive information from the carriers had disclosed customer information to others, 555 F.3d at 1001, much as the data miners here argue that they receive only "de-identified" information from pharmacies. The D.C. Circuit retorted: "This argument . . . performs a sort of sleight of hand. It diverts attention from the fact that the carrier's sharing of customer information with a joint venturer or an independent contractor without the customer's consent[16] is itself an invasion of the customer's privacy – the very harm the regulation targets." *Ibid.*

So too here. The data-mining plaintiffs and the pharmaceutical industry association plaintiff seek to divert attention from the fact that the pharmacies' sharing of customer information without consent is the crucial privacy invasion. It is quite unclear, and in the view of amicus doubtful, that the plaintiffs' supposed de-identification actually protects patients from being identified. And "[e]ven if there were no possibility that

16. Admittedly, Vermont's law does not require patient approval, as would be required for perfect symmetry. But we do not understand either the Second Circuit's analysis or the plaintiffs' position to mean that the First Amendment defect of Vermont's law is its reliance on prescribing physicians for protecting patients' privacy, rather than patients themselves.

a patient's identity might be learned from a redacted medical record, there would be an invasion of privacy." *Northwestern Memorial Hospital v. Ashcroft*, 362 F.3d 923, 929 (7th Cir. 2004) (analogizing disclosure of de-identified medical records to disclosure of de-identified nude pictures).

The D.C. Circuit went on to reject the carriers' commercial speech arguments. It recognized that "common sense supports the … determination that the risk of unauthorized disclosure of customer information increases with the number of entities possessing it." *NCTA*, 555 F.3d at 1001-02. And it found that the FCC "reasonably concluded that customer information would be at a greater risk of disclosure once out of the control of the carriers and in the hands of entities not subject to § 222." *Id.* at 1002. This reasoning fully applies here. Limiting pharmacies' disclosure of PI data reduces the risk that patients' privacy will be violated.

In short, Vermont's Prescription Confidentiality Law is like the FCC order challenged in *NCTA*: in both cases, Congress statutorily recognized a substantial privacy interest for customer information considered to be sensitive, established that consent mechanisms advanced that privacy interest, and authorized the FCC in one case and the states in the other to elaborate on the implementation of consent mechanisms.

B. The Court of Appeals' analysis threatens many other privacy laws.

HIPAA is but one of a number of important federal privacy statutes that address a fundamental reality of modern life: that we disclose much personal information about ourselves to others, either as part of a direct transaction, or because we need an intermediary or third party to communicate or transact. Many of these statutes would be vulnerable if the Second Circuit's analysis were correct.

Federal telecommunications law has long protected the privacy of communications and communication records. One purpose of the Wiretap Act is "to protect effectively the privacy of wire and oral communications." *Bartnicki*, 532 U.S. at 523 (citation omitted). Similarly, the Stored Communications Act generally prohibits providers of electronic communications service and of remote computing service from disclosing the content of users' communications, but permits such disclosure with the consent of the user or subscriber. 18 U.S.C. § 2702 (2010); *see* S. Rep. No. 99-541, at 3, *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557 (the Stored Communications Act's purpose is to "protect privacy interests in personal and proprietary information, while protecting the Government's legitimate law enforcement needs."); *see also* Cable Communications Privacy Act, 47 U.S.C. § 551(c)(1) (2010) (prohibiting disclosure of "personally identifiable information" concerning cable subscriber without consent).

The Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.* (2010), prohibits consumer-reporting agencies from disclosing credit reports except in delineated circumstances; these restrictions do not violate the First Amendment. *Trans Union Corp. v. FTC*, 267 F.3d 1138 (D.C. Cir. 2001), *denying reh'g in* 245 F.3d 809 (D.C. Cir. 2001). The Right to Financial Privacy Act, (RFPA), 12 U.S.C. § 3401 *et seq.* (2010), prohibits banks, building and loan associations, and credit card issuers among others, *id.* § 3401(1), from disclosing financial records to the government except under specific circumstances, such as where the customer authorizes the disclosure, or the government obtains a warrant, *id.* § 3402. *See also, e.g.*, Gramm-Leach-Bliley Act, 15 U.S.C. § 6802(b) (2010) (financial institution customers' right to opt-out of disclosure of personal information); Driver's Privacy Protection Act, 18 U.S.C. § 2721 *et seq.* (2010 (restricting disclosure of driver information without consent); Video Privacy Protection Act, 18 U.S.C. § 2710(b) (2010) (prohibiting disclosure of "personally identifiable information concerning" consumer of video rental establishment without consent).

These statutes strive to balance this reality of personal information dissemination in an age of sophisticated and cheap computer technology with society's reasonable expectations of privacy and confidentiality. Under the Court of Appeals' analysis, however, all of these statutes may be unconstitutional.

Finally, the scope of the analysis below threatens more than current federal privacy law. Many privileges, most of which are codified by statute and all of which are designed to facilitate communication among private parties, are

equally vulnerable. The attorney duty of confidentiality and the psychotherapist-patient confidentiality obligation, applying to only certain categories of communications, are two obvious examples that ordinarily satisfy the First Amendment. *See Aguilar*, 515 U.S. at 605 ("As to one who voluntarily assumed a duty of confidentiality, governmental restrictions on disclosure are not subject to the same stringent standards that would apply to efforts to impose restrictions on unwilling members of the public."); *American Motors Corp. v. Huffstutler*, 575 N.E.2d 116, 120 (Ohio 1991) (enforcing attorney-client privilege against person who voluntarily submits to state licensing to be an attorney does not violate the First Amendment).

Businesses should be wary, too. In particular, the Uniform Trade Secrets Act (UTSA) prohibits disclosure of a trade secret by one who obtains it through a confidential relationship such as employment, regardless of whether there is an express contract protecting such information. Unif. Trade Secrets Act § 1, 14 U.L.A. 433 (1985); *see, e.g.*, *Expo Chem. Co. v. Brooks*, 572 S.W.2d 8, 12 (Tex. Civ. App. 1978) (explaining that no contract is needed to impose a duty on an employee to refrain from disclosing or using the employer's trade secrets). Many trade secrets, such as the results of a proprietary study on the side effects of a new drug, could easily be a matter of public concern—unlike the PI data here. State trade secret laws may thus be vulnerable to First Amendment challenge under the analysis below.

Each of the foregoing federal and state statutes and privileges would be vulnerable to attack under the Court of Appeals' analysis. The First Amendment does not require the sacrifice of our privacy to promote data

exchanges that benefit only commercial speakers and their specific business audiences.

CONCLUSION

Amicus respectfully urges this Court to reverse the decision below.

Respectfully submitted,

Cindy Cohn
Counsel of Record
Lee Tien
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
(415) 436-9333
cindy@eff.org

Attorneys for Amicus Curiae
Electronic Frontier Foundation