TRANSCRIPT: *SORRELL V. IMS HEALTH*— ANY IMPACT ON PATIENT PRIVACY?

John Verdi[*†]

My name is John Verdi. I work at the Electronic Privacy Information Center. I just want to be clear up front: At EPIC, our interest in *Sorrell*[1] was in patient privacy. The physician-privacy aspect of this case, the high-cost-of-brand-name-pharmaceutical aspect of this case, the anti-detailing aspect of this case, these are all interesting issues, no doubt, but they are issues on which we do not have any particular expertise in my organization. We do have some amount of expertise concerning patient privacy and consumer privacy, so those are the issues to which we restricted our brief, and those are primarily going to be the issues that I'm going to talk about today, although I'm happy to take questions on whatever.

The first question I think that needs to be asked is: What does the decision of *Sorrell* mean for consumer-privacy statutes generally? We've heard a lot today that got at that question in a variety of different ways, but I'm going to suggest something that I think might be provocative and, my genuine view is, that it doesn't mean much at all. I think that it is pretty clear that the Supreme Court in this case viewed the Vermont statute at issue as not a consumer-privacy statute. At maximum it was a physician-privacy statute, not a patient-privacy statute, and I think that there are ample clues in the majority opinion that presage how the Court would differently treat a genuine patient-privacy statute here. The Court was extremely skeptical that the Vermont law really was focused on patient privacy. I think some of that had to do with the legislative record at issue here. I think some of it had to do with the actual terms of the statue. And from our perspective at EPIC, we viewed it as a patient-privacy statute in many ways—an imperfect one no doubt—but a patient-privacy statute.

So why did we file a brief in this case if we were focused on patient privacy and a number of Supreme Court Justices who are much smarter than we are at our little organization decided that this was not a patient-privacy statute at all? Well, we were very much concerned that the Court would view this as a patient-privacy statute and would nonetheless hold that the patients' privacy interests were not a compelling state interest under their First Amendment jurisprudence. And our fear was that if that happened, all manner of consumer-privacy laws were either dead letters or

---

* General Counsel, Electronic Privacy Information Center.

† Please note that the Speaker reviewed and edited this Transcript. Language added by the *Vermont Law Review* appears in brackets, and ellipses indicate omissions of language.

1. Sorrell v. IMS Health Inc., 131 S. Ct. 2653 (2011).

on the chopping block, and we did not want to see that happen. So what we attempted to do was highlight the consumer-privacy interests, the patient-privacy interests that were at issue in the statute. And why did we think that there were clear patient-privacy interests here if, by all accounts the most identifying information about patients, the patients' names, was redacted from the records at issue and the data that was transferred?

We believe patients' privacy interests were at stake because we do not think that those records were sufficiently de-identified. We believe that there is ample evidence, both from a technological perspective and from a sociological, data-driven, re-identification perspective, that those records—even though the names were turned into unique identifiers that were no longer first-name, last-name pairs—that those names could be recreated, either through cracking the MD5 hash that was the cryptographic technique that was used to obscure this information and assign the unique identifier, or through re-identification techniques based on the inherent personalization of medical records. The reality of this is that medical records contain lots of information about location, gender, medical conditions, age, date of birth, year of birth, that when taken together and when ample computing power is applied, can be used to re-identify patients. And that is the core concern, from our perspective, at the heart of the case. Now I think the reality is, based on the majority decision, that the Court did not agree with us. The Court believed that the patient data was sufficiently de-identified and the Court's view was that even if it was not, the patients' privacy interest was not targeted by the Vermont statute at issue. So that is why I believe that *Sorrell* doesn't have much to say at all, moving forward, about consumer-privacy statutes. I do not think it has much to say about the Driver's Privacy Protection Act,[2] [and] I do not think it has much to say about the Video Privacy Protection Act.[3] In fact, I don't think it has much to say about HIPAA.[4] Flawed though HIPAA may be, there are in fact privacy provisions in there, and my sense is that *Sorrell* does not call into question the legitimacy of those provisions.

Now, why does the question that we briefed matter before the Court? Why does it matter whether or not the Court would view consumer privacy as a compelling state interest? We think that this question matters because increasingly things that used to be real-world, physical-world business practices, things that used to record data in a physical space and involve a transfer of physical records, are increasingly being moved to the digital

2. Violent Crime Control and Law Enforcement Act of 1994, 18 U.S.C. § 2721 (2006).

3. Video Privacy Protection Act of 1988, 18 U.S.C. § 2701 (2006).

4. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified in scattered sections of 18, 26, 29, & 42 U.S.C.).

space. They are increasingly becoming data flows. And from our perspective, that is what this case was all about. It was about the data flow from the pharmacy to the data broker. That is an automated data flow based on the systems that are in place that happens without any meaningful consent by the patient, without any meaningful action by the pharmacist, and without any meaningful burden on the data broker. Once these systems are established, the data flow simply happens.

Now, what do I mean when I say that practices in physical space are essentially transitioning into these data flows? For example: Psychiatrists routinely take notes concerning their treatment of patients. Some individuals, rather than going to a psychiatrist in 2011, are participating in online forums—in mutual support bulletin boards—concerning their mental health conditions. Records of their participation there is a data flow that is saved by innumerable companies and actors within that transaction—the ISPs that are hosting the site, the company that provides the bulletin board, [and] potentially the company that provides authentication for that system. So that has now become a data flow, and if the Supreme Court looks at these cases broadly and says that consumer privacy is not a compelling state interest that legislatures are free to protect through legislation, any laws that would restrict the disclosure of that sort of mental health information get called into question.

Prescription records . . . are now becoming, in many ways, also identifiable to individuals when they go on the web and they search for side effects and they plug in drug names on websites and those searches can then be tied back to them. Video store rental records—you used to have to go to a video store, I'm sure some people here remember video stores—Blockbuster, others, anybody? Those records are just data flows from your YouTube account and your Hulu account to an advertiser and a marketer at this point, and a data broker. Driver's license data, which typically sits at the state DMV or the state RMV, that is now becoming a data flow from your insurance company which has all your personal driving information, the same as the state DMV does. And that is becoming a data flow from the insurance company to data brokers and others. Library records—there are lots of strong state laws that protect the privacy of library-borrowing records. Well guess what? As the Google Books settlement moves forward, as other similar structures move forward for digital libraries, your borrowing history, your reading history, your annotations on your Kindle and your Nook and your iPad: They are just data flows. And the question is: is the protection of privacy of those data flows, for consumers, a compelling state interest? And that is a question that *Sorrell* leaves absolutely open, to my mind.

I am going to identify a couple of problems that arise out of these increased data flows. The primary problem is that as companies are collecting ever more data about individuals, as that collection is becoming ever more automated and ever more identifiable to individuals, individuals' technical and practical capacity to limit that disclosure and control their own information is becoming absolutely destroyed. It used to be—when I began surfing the web in 1996, I'm sorry, I know that makes me very old—but it used to be that I could make a couple small changes to my browser settings about whether or not I accept cookies [or] about whether or not I enable technologies like Java and Java Script . . . that could largely protect me from any online tracking that was going on; it was fairly unsophisticated at that point in time.

The reality today, and there is ample research in the technical community to demonstrate this, most recently being a very good study published by one of the Stanford clinics that came out last week, about what is essentially rampant tracking of individuals across the internet by the top internet sites.[5] You can also see reporting on this in the *Wall Street Journal* last year;[6] you see a number of technical papers that have been published in the last decade about this. This sort of tracking is becoming increasingly automated and it is becoming increasingly difficult for consumers to stop or to even control. I would simply note a couple of things. First, we had flash cookies, which are bits of data on your computer that can track you across the web and are slightly more difficult to delete than regular cookies. Then we had zombie cookies, which are apparently flash cookies that have an appetite for human flesh. Then we have use of the HTML 5 data cache. Is anyone glazing over yet? I used to build secure web applications before I became a lawyer; I glazed over at zombie cookies. This is not even to speak of Facebook's off-site cookie tracking, the Stanford study that talked about passing user IDs in URL query strings, deep-packet inspection by Internet service providers, and beacon technology that's used on these websites.[7] Really, are all of your eyes glazing over at this point? Consumers simply have no practical way to control these data flows and control the record of their own data.

---

5. Jonathan Mayer, *Tracking the Trackers: Where Everybody Knows Your Username*, STANFORD L. SCH. CTR. FOR INTERNET AND SOC'Y (Oct. 11, 2011, 8:06 AM), http://cyberlaw.stanford.edu/node/6740.

6. Throughout 2011, the *Wall Street Journal* published a series of articles grouped under the heading "What They Know." *The Original Series*, WALL ST. J., http://online.wsj.com/public/page/what-they-know-digital-privacy.html.

7. Mayer, *supra* note 5.

So what do they need? They need lawmakers like Sharon and like some of our friends in Congress to implement legal protections. A technological arms race does not work for consumers; it is destined to be a total failure from the consumer perspective. So you need clear legal standards and clear meaningful legal protections that have to do with notice, consent, meaningful consent, opt-in, opt-out. All of these structures are in play and I think that all of these possibilities exist after *Sorrell*. I do not think there is any question.

I will close with two things. One, I will note an oddity; second, I will tell a joke. First, the oddity. The oddity is that in *Sorrell*—and this may be because I am right in my analysis, though do not trust me on that, it may be for another reason—the oddity in *Sorrell* is that [it] essentially evades a very interesting question that was raised in the dissent in the Second Circuit level,[8] and that is a line-drawing question. If these data flows are speech and there is a specific focus on the data flow from the pharmacist to the data broker and from the data broker to the pharmaceutical company and then from the pharmaceutical company to the doctor: That is a line-drawing issue. Why don't we push that line temporally a little bit further back?

And let's talk about the data transfer from the patient to the pharmacist. That is a compelled disclosure; it is compelled under state law. It is a state law that says I cannot get Vicodin unless I have a prescription. That is not a natural law; I am not Thomas Aquinas and neither is Congress. (That was not the joke by the way.) This is a federal law, interacting with state statutes that require [that] I not have access to certain pharmaceuticals without a prescription. Let's push the line further back. The doctor had a data flow to the patient and wrote me a prescription. That is free speech, too. So one of the things that the Supreme Court really does not get into—and I think it is because they simply did not view this as a patient-privacy statute at all—they do not get into the very clear doctrinal First Amendment interests in those two data flows. And I have got a hint for you guys: Those doctrinal interests, those First Amendment interests, conflict with the data brokers' interest in this case and you have a war between First Amendment interests. Number one, there is a clearly established constitutional First Amendment right to speak anonymously.[9] Both of those laws—the law that requires the doctor to write me a prescription and the law that requires me to present a

8. INS Health Inc. v. Sorrell, 630 F.3d. 263, 282 (2d Cir. 2010) (Livingston, D., Circuit Judge, dissenting).

9. Talley v. California, 362 U.S. 60, 64 (1960); McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 341–42 (1995) ("The decision in favor of anonymity may be motivated by fear of economic or official retaliation, by concern about social ostracism, or merely by a desire to preserve as much of one's privacy as possible.").

prescription to my pharmacist—invade my First Amendment right to speak anonymously. I ought to be able to fill prescriptions anonymously based on this constitutional standard. If that is speech—I doubt that it is, but Justices on the Supreme Court disagree with me—if those data flows are speech, I have a right to express that speech anonymously.

Secondly, there is a clear right to receive information anonymously and to read anonymously under the First Amendment.[10] And when you go back to all the consumer privacy laws that I just talked about that impact tracking on the web, tracking of your library reading, tracking of your other purchases, those business practices invade and those laws seek to control my right to receive information anonymously. So now you have a genuine battle between First Amendment interests. And I do not know how this battle turns out. I do not know which way it goes, and I do not know, frankly, whether the battle is going to be adjudicated by the Supreme Court at all because I do not know how seriously to take the Court's position that these data flows really are speech. But assuming [that] they are, those real, genuine conflicts are built in. That is the oddity that I would like to observe.

Now my joke. I understand that folks have tried to make distinctions here today between beef jerky, widgets, and free speech. I can tell you I do not have any experience with widgets. I do have experience with beef jerky. And God knows—you have been listening to me for the past fourteen minutes—I have experience with speech. I can tell you one thing that I do know: Every encounter I have ever had with beef jerky has been delicious. That is not true of speech. Thank you.

---

10. *E.g.*, Bd. of Educ. v. Pico, 457 U.S. 853, 867 (1982). "[T]he right to receive ideas follows ineluctably from the *sender's* First Amendment right to send them . . . . More importantly, the right to receive ideas is a necessary predicate to the *recipient's* meaningful exercise of his own rights of speech, press, and political freedom." *Id.*; Stanley v. Georgia, 394 U.S. 557, 565 (1969) (striking down a criminal prohibition on private possession of obscene materials as inconsistent with "the right to be free from state inquiry into the contents of [one's] library"); *see also* Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981, 1007–12 (1996) (reviewing court decisions recognizing or implicitly relying on a right to receive information anonymously).