OREGON'S VISION FOR PRIVACY PROTECTION AND ENFORCEMENT

HONORABLE ELLEN F. ROSENBLUM*
OREGON ATTORNEY GENERAL

PRIVACY LAW SYMPOSIUM KEYNOTE ADDRESS | FEBRUARY 26, 2016

Editor's Note: *This address was given to the attendees of Willamette Law Review's Annual Symposium on February 26, 2016, focusing on Privacy and Data Security Law. It is preserved in its original form.*

Thank you to Willamette University's College of Law for hosting today's symposium. It's really important for you to be bringing attention to this topic, and you've assembled a tremendous group of speakers, as well as a remarkable group of lawyers and others in your audience. I genuinely appreciate the invitation to join you.

Discussions of data security often focus on the private law arena—privacy, data security harms, litigation trends in data breach cases, workplace privacy and data breach, managing risks through cyber insurance policies, and data sharing issues—however, this discussion will focus more on the public side of this new era of data breach and cybersecurity—certainly a "full-employment act" for the legal profession! On my watch, the Oregon Department of Justice has been paying closer attention. We've held a national symposium on online privacy. We've trained thousands of seniors—who love their computers—in how to avoid online scams. We've worked with the legislature in developing and getting passed into law cutting-edge privacy-related policies while trying to protect Oregonians, especially our children and our seniors. Most recently, I've created a new unit within the Department of Justice, with four of our best and brightest lawyers; it's called the Online Consumer Privacy Unit.

My experience at the Department these past four years has taught

*Retired Judge of The Oregon Court of Appeals

me some very basic lessons which, though fairly simple and unsurprising, bear repeating today before I delve a little more deeply into what we are doing.

First, we need to focus more on the criminal aspects of the stealing and misuse of data. It's theft of our identities, an insult and affront to our dignity and to our sense of who we are. In other words, it's not just another casualty of our modern technological era. Though data theft doesn't carry with it the same sense of violence a person may experience when she's robbed or her house is burglarized, it's still a crime—not an abstraction. So we need to address internet crime for what it is. It takes a real effort to build this awareness. As all of you know, the consequences of having your information stolen can be devastating. I want everyone to understand the seriousness and the outright illegality of these acts.

Second, cybercrime is one of the toughest crimes to prove. The perpetrators usually are far away and have covered their tracks effectively by the time their acts become known to their victims.

This leads to my third basic premise: we're far better off taking actions that will help to prevent cybercrime and other forms of data invasion in the first place. So, as with most areas of consumer protection, education and prevention have to be at the top of our lists. In most instances, data breach and identity theft can be avoided in the first place, so we need to emphasize ways to achieve that.

Finally, as computational power expands and inventors and engineers come up with all manner of new uses of digital devices, the challenges that face us grow greater every day. Just take one new development: driverless cars. Then, multiply by the thousands of new ways data is being captured and used and by the many, many new developments of our era—culminating in the Internet of Things. Is this a good *thing* or a bad *thing*? Hopefully, it's the former—but not if it compromises our privacy to an unacceptable, and perhaps even an unknowable, degree.

A column in the Business Section of *New York Times* provides perfect context for today's symposium. It says:

> [H]ere's one bet you'll never lose money on: Digital technology always grows hungrier for more personal information, and we users nearly always accede to its demands. Today's smartphones hold a lot of personal data—your correspondence, your photos, your location,

> your dignity. But tomorrow's devices, many of which are already around in rudimentary forms, will hold a lot more.[2]

Let me use a car analogy to help get us centered. A hundred years ago, it was estimated there were just under 5 million cars on the roads in our nation.[3] During that time, car usage was almost doubling every two years.[4] Talk about rapid expansion! Here's a picture of a road in 1919. It's almost impassable and certainly not convenient or safe.

[5]

2. Farhad Manjoo, *The Apple Case Will Grope Its Way into Your Future*, N.Y.TIMES, Feb. 24, 2016, http://www.nytimes.com/2016/02/25/technology/personaltech/the-apple-case-will-grope-its-way-into-your-future.html?_r=0.

3. Richard F. Weingroff, *Vol. 1, No. 1—The First Issue of Public Roads, May 1918*, U.S. DEPT. OF TRANSP. (May–June 2000), https://www.fhwa.dot.gov/publications/publicroads/00mayjun/volume1.cfm ("The article by highway engineer Andrew F. Anderson reported that 4,983,340 motor cars, including commercial vehicles, and 257,522 motorcycles were registered in 1917.").

4. *Id.* ("The United States' total represented a 44-percent increase over 1916, an increase that was approximately the same as in each of the previous five years.").

5. *Washington-Richmond Road*, NATIONAL MUSEUM OF AMERICAN HISTORY (1919), http://amhistory.si.edu/onthemove/collection/object_488.html.

Now, here is the same road in 1947. Notice what a difference thirty years can make.

 [6]

What did it take to get from a muddy mess that frustrated everyone to smooth pavement? I would speculate it took a lot of smart people, sound policy, and industry expertise to tackle this broad and sticky issue.

Here we are again, one hundred years later, with astronomically growing fields in technology. Big Data has helped us combat the flu, helped children learn, and helped businesses grow. The internet of things can make our cars safer and make our busy lives freer to focus on priorities. But some of these rapid changes have left privacy—a central feature of our liberty—looking more like that messy, muddy road. They also have left us more open to exploitation.

With that as context, let me talk a little more specifically about what the Oregon Department of Justice is doing to try to look out for the rights and interests of average Oregonians in this increasingly complex arena. I'll start with basic data breaches and work my way through to legislation our department has promoted and actions we're

6. *Washington-Richmond Road*, NATIONAL MUSEUM OF AMERICAN HISTORY (1947), http://amhistory.si.edu/onthemove/collection/object_490.html.

taking.

Data breaches, as we know all too well, are an increasingly common menace to a lot more than branches of government. No one is immune. They hit grocery stores, hospitals, schools, state agencies, online vendors—really, any organization that stores valuable personal information. According to the Identity Theft Resource Center, in 2015 there were 781 data breaches.[7] This represents the second highest year on record since the Identity Theft Resource Center began tracking breaches in 2005.[8] The more I learned about the increasing risk of identity theft to Oregonians, the more I wanted to know if the laws enacted to protect them years ago are still sufficient today.

It was against this backdrop that I set out to review the adequacy of our fundamental data breach law, the Oregon Consumer Identity Theft Protection Act, originally passed in 2007.[9] I worked with consumer advocates, polled other Attorneys General, and worked with retailers, hospitals, and others to create a bipartisan-supported update to this law.

Our data breach law has two primary functions. First, it says that if personal information is breached, the breached company must give timely notice to those affected.[10] This helps consumers take proactive steps to be on guard against identity theft. Second, the law requires those who keep personal information to maintain reasonable security measures to protect it.[11]

Like most data breach statutes of its vintage, Oregon's was concerned mostly with financial information—credit cards, social security numbers, and bank accounts. Nearly a decade later, we found that both the targets and consequences of data breach are far more extensive than they used to be. The most significant personal information not protected under Oregon data breach law was medical information. The Ponemon Institute, which conducts independent research on privacy, data protection, and information security policy recently released its fifth annual study on privacy and security of healthcare data.[12] It found that medical identity theft has nearly

7. *Identity Theft Resource Center Breach Report Hits near Record High in 2015*, IDENTITY THEFT RESOURCE CENTER (2016), http://www.idtheftcenter.org/ITRC-Surveys-Studies/2015databreaches.html.

8. *Id.*

9. OR. REV. STAT. §§ 646A.600–628 (2015).

10. *Id.* § 646A.604.

11. *Id.* § 646A.622.

12. *Fifth Annual Study on Medical Identity Theft*, PONEMON INST. (2015),

doubled in the last five years, with victims spending an average of $13,500 apiece to restore their credit, reimburse their healthcare provider for fraudulent claims, and correct inaccuracies in their health records.[13]

Another area not covered under the original 2007 bill: biometric data—that is, any data about your physical attributes: facial features, retina scans, fingerprints, etc. More and more biometric information has the potential to be stolen. Many of us use our fingerprints to unlock our phones. This means fingerprint information could be the subject of a breach. In December of 2014, a group called the "Chaos Computer Club" succeeded in recreating the fingerprint of a German Defense Minister using nothing but readily available technology and high-definition photos.[14] So, vulnerability clearly exists. And unlike the password to your bank account, you cannot change your biometric information. It follows you everywhere! I worried about what could happen if we fail to take steps to protect this information now.

Oregon's new law, effective as of January 2016, adds health insurance, medical, and biometric information to the definition of "personal information"—that is, information that must be reasonably protected under Oregon law.[15]

In my overview of the data breach statutes, I learned that in 43 of the other 47 states, which have some form of statutory data breach protection, jurisdiction rests with the Attorney General.[16] This, in turn, allows most national scale data breaches to be dealt with at the national level, where there is a special working group dealing with data breach. Before the new law, our existing framework had only the Department of Consumer and Business Services (DCBS) in the role of enforcer. Oregon could not take the lead on multi-state investigations, and DCBS does not have the authority to work within this group. Without Attorney General enforcement, we were often on the outside looking in. The second major part of the bill is that enforcement authority has been extended to the Attorney General to allow Oregon to sit as a full partner in the national discussions around data breach. And let me assure you: we are taking full advantage.

---

http://medidfraud.org/wp-content/uploads/2015/02/2014_Medical_ID_Theft_Study1.pdf.

13. *Id.*

14. Zoe Kleinman, *Politician's Fingerprint 'Cloned from Photos' by Hacker*, BBC NEWS, Dec. 29, 2014, http://www.bbc.com/news/technology-30623611.

15. OR. REV. STAT. § 646A.602(11) (2015).

16. *See generally* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS 173-74 (2d ed. 2013).

The third major update to the data breach law requires that notice be given to the Attorney General when a large breach occurs. By "large," I mean a breach that affects 250 or more Oregonians. Many states already require this, and it makes a lot of sense. When a breach happens, it's important that impacted consumers know about it. That's already the law. But what was missing was any requirement that state government be alerted. Without such notice, we struggle to spot trends in data breach, weaknesses in our own laws, and to help consumers distinguish between an authentic breach notice versus a fraudster phishing for their personal information.

To help get the word out, we also made a website for data breach issues. Its URL is https://justice.oregon.gov/consumer/DataBreach. The site has two pages: one focused on companies that need to report a breach; the other, focused on consumers who were victimized by a breach. The reporting companies can simply upload a copy of their breach notification, fill in some information about the breach, and submit their notice to my office. Once cleared through our processing system, the breach notification letter is placed on the consumer-facing page so that consumers can make sure the breach letter they received is the real letter they should respond to. Breached companies will often accompany their notification with an offer for free credit monitoring that requires a consumer to turn over more personal information—something which a recently-breached consumer might be, understandably, quite leery of doing!

I want to talk about another very important policy issue related to privacy of which I am very proud. This pertains to one special group of vulnerable Oregonians and will have an important impact on the privacy world in the decades to come: our K–12 schoolchildren.

You know the old saying: "Grades follow you forever." Well, as recently as ten years ago, that didn't mean much more than a manila folder in a drawer. Requesting a transcript was something you did by mail. But now it's not just grades that can follow a student; as educational curricula move further into the cloud, more and more of our children's daily activities are being recorded and tracked.

Today, many schools and teachers use software and other online tools to help track student grades, preferences, homework, and progress. These tools are extremely helpful to students, parents, and teachers, but if the data is used inappropriately, the online records can follow a child throughout their life. Some of the collection of data is already protected by the Family Educations Rights and Privacy Act (FERPA) of 1974, which prohibits the disclosure of standardized test

scores, disciplinary history, and other official student records. But FERPA does not protect other student online data.

A student's data is of tremendous value to educators, allowing them to better identify students who might be struggling in a particular subject. But all of this data also has real commercial value: it can be used to target ads to the students and their families, or to build profiles with the potential to follow students from K-12 and beyond. Some tech companies can collect millions of data points a day on a child, and that information needs to be protected.

This is where Oregon Student Internet Privacy Act (OSIPA) enters the scene.[17] At its core, OSIPA is very simple: it ensures that K-12 student's personal information that is gathered by educational technology companies while the students are in the classroom may be used for educational purposes only. It forbids these companies, which contract with school districts, from using the students' data to create marketing profiles and from selling data to advertisers or marketers. Keep in mind, this data includes everything from the family's socioeconomic information, to grades, to what the child chooses for lunch in the cafeteria.

To be clear, the educational benefits of EdTech promise to be significant and I am all in favor of the proper use of student data to help our children learn. That is why I developed OSIPA in consultation with educators, teachers, industry experts, and privacy advocates. But our school children should be given every opportunity to succeed in the classroom without exploitation of their personal data. And parents should be able to send their children to school without having to worry about intrusions into their family's privacy.

Now back to those muddy roads for a minute: self-driving cars, or autonomous vehicles, may be the greatest disruptive innovation to travel that we have experienced in a century. Already, regulations are being formulated in places like California and Canada. Oregon just hired an expert at the Department of Transportation to focus on development of our own autonomous vehicle regulations. And earlier this month, I coordinated a panel entitled "Cars, Cars, Cars" for the American Bar Association's midyear meeting in San Diego.[18] The panel explored emerging issues facing lawyers in the world of cars,

17. OR. REV. STAT. § 336.184 (2015).

18. *See 2016 ABA Midyear Meeting, San Diego, CA*, A.B.A. SEC. ST. & LOC. GOV'T L., Feb. 4, 2016, http://www.americanbar.org/groups/state_local_government/events_cle/2016-aba-midyear-meeting—san-diego—ca.html.

not just self-driving cars. The conversation was fascinating. Panelists discussed everything from copyright issues relating to the software in vehicles to drafting regulations allowing autonomous vehicles to safely share the roadways with traditional drivers, as well as the (often undisclosed) gathering of data by manufacturers, which can include everything from where and how a consumer drives to how frequently they stop for coffee or talk on the phone while driving.

In the new "Internet of Things," everyday objects have network connectivity, allowing them to send and receive data. It may sound great, but, to be honest, I worry it could be a privacy nightmare. To put this another way: I assume we all continue to value the notion that our home is our castle. But what would happen if the Internet of Things made that home more like a prison, including 24-hour surveillance? The battle between Apple and the FBI over cracking open a terrorist's smartphone will certainly have repercussions for the future of the tech industry. It certainly is a tipping point in the discussion of our own sense of privacy and personal security.

I want to close by thanking you for your interest and involvement in this fascinating emerging area of law. If you are a student here today, you need go no further to find a niche practice area! The American Bar Association's model rules of professional conduct for lawyers make it a duty for lawyers to keep abreast of the benefits and risks associated with technology.[19]

I hope you can see that protecting the privacy and security of Oregonians has been an important goal for me as Attorney General. We've already made some great progress, but just like the people 100 years ago who gave their time and efforts to make muddy roads smooth, we need to work together to frame privacy law and protect Oregonians in this regard for generations to come.

Thank you. I look forward to working together.

19. MODEL RULES OF PROF'L CONDUCT R. 1.1 cmt. 8 (1983).