Susan Landau
Tufts University[1]

Hearing of the Joint Committee on Advanced Information Technology, the Internet and Cybersecurity
Testimony on the Massachusetts Data and Digital Privacy Act (H. 83/S. 25)

October 19, 2023

Thank you for the opportunity to offer testimony about the Massachusetts Data and Digital Privacy Act.

I have studied and written about the security and privacy of communications systems for over thirty years. My scholarship has often focused on public policy issues, and thus, I have testified before the U.S. Congress and served on study committees focusing on privacy issues for the National Academies of Science, Engineering, and Medicine, the Carnegie Endowment for International Peace, and other organizations.

I am the Bridge Professor of Cyber Security and Policy at The Fletcher School and the School of Engineering, Department of Computer Science at Tufts University, where I teach and do research in cybersecurity, national security, law, and policy. I am also founding director of our MS degree in Cybersecurity and Public Policy. Much of my work focuses on communications security and privacy. Prior to my tenure at Tufts University, I was Professor of Cybersecurity Policy at Worcester Polytechnic Institute, Senior Staff Privacy Analyst at Google, and Senior Staff Engineer and Distinguished Engineer at Sun Microsystems. I have also held academic positions at the University of Massachusetts and at Wesleyan University. I hold a PhD in applied mathematics from MIT, an MS from Cornell University, and a BA from Princeton University. As you can see, I have spent almost all my career in Massachusetts.

I am here to strongly support the passage of the Massachusetts Data and Digital Privacy Act (H. 83/S. 25). I want to speak on the importance of Section 2, which minimizes the use of information collected from users. Such protections are very badly needed.

I will focus my remarks on smartphone communications metadata and software and device telemetry. This is because the information supplied by this data allows for detailed profiles of users—and yet the users can do nothing about the data collection and use.

Almost all of us carry smartphones with us most of the day (and some even from the moment they wake up til they go to bed). We have all been educated about how the information we provide to the device—requests for directions, searches, etc.—can be shared widely. But there is lots of other information that we unknowingly provide and, thus, whose use we cannot control. Communications metadata and device and software telemetry can reveal intimate information

[1] Bridge Professor of Cyber Security and Policy, The Fletcher School and School of Engineering, Department of Computer Science, Tufts University, 160 Packard Ave., Medford, MA 02155. susan.landau@tufts.edu. Affiliation is for identification purposes only.

about how we spend our days: where we are, what we do there, and with whom. The information derived from this data can give its recipients—operating systems, ISPs, apps, and data brokers—detailed profiles of our health, our finances, our interests, and much, much more[2]—and, as the Federal Trade Commission and others have noted, may be used in ways that harm users.[3]

Now, it is not new to collect such information. From its earliest days, the regulated telephone monopoly, AT&T collected and measured trunk traffic to determine how its services were working and to project future usage; the company also recorded customer use of the system for billing purposes. Decades later, the company used communications metadata to uncover customer fraud. The ending of AT&T's monopoly created competition in Public Switched Telephone Network (PSTN); and telephones companies began Call Detail Records—who called whom when and for how long—to lure customers by offering them better deals on calling their "friends and family." This was the beginning of use of communications metadata for advertising.

The Internet made communications metadata richer and more valuable. The PSTN is effectively a voice communication channel, while the Internet allows for many different types of communication, including email, Voice over IP (VoIP), photos, video, etc. This is enabled by the Internet Protocol (IP)—and that means that IP communications metadata includes richer detail about a user's activities than the Call Detail Records of the PSTN.

That was not the only change in our communications modalities; the other, occurring essentially simultaneously, was our move to mobile phones. Where someone goes can be really revelatory about their interests, behaviors, intents, and character. With mobile phones, which users carried with them day and night, that information became available to service providers.

The communications revolution did not end there. Cellphones became smartphones. Information about a user's location was transmitted not just to the service providers that connected the call but also to the phone operating system, the apps, and data brokers.

The data collection did not stop there. Smartphones acquired sensors, including accelerometers, gyroscopes, magnetometers, proximity sensors, ambient noise sensors, and power sensors; these enabled the devices to display their content no matter which way they are held. They let a user hold her phone to her ear and not accidentally activate other apps, learn when the phone battery is running low, use her phone to navigate a new city or simply her commuting route—and use the millions of apps that were not imagined seventeen years ago when the iPhone made its debut.

Communications metadata and software and device telemetry can also be used for other purposes.

[2] This information is derived from Susan Landau and Patricia Vargas Leon, "Reversing Privacy Risks: Strict Limitations on the Use of Communications Metadata and Telemetry Information," *Colorado Technology Law Journal*, Vol. 21, Issue 1 (2023), pp. 225-336.

[3] See, e.g., Federal Trade Commission, "A Look at What ISPSs Know About You: Examining the Privacy Practices of Six Major Internet Providers," (2021), https://www.ftc.gov/system/files/documents/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major-internet-service-providers/p195402_isp_6b_staff_report.pdf and See, e.g., Andreas Claesson and Tor E. Bjorstad, Norwegian Consumer Council, "Out of Control: A Review of Data Sharing by Popular Mobile Apps," (2020), https://fil.forbrukerradet.no/wp-content/uploads/2020/01/mnemonic-security-test-report-v1.0.pdf

The information of what number or IP address we communicated with, when, and for how long, is important to service providers for billing, provisioning service, planning future service, and fraud detection. It also provides a social profile of us: who we're connected with, how intensely, etc. Combining that with outside information can be highly revelatory of a person's intentions.[4]

Device telemetry—accelerometers, gyroscopes, magnetometers, battery sensors, etc.—are extremely useful on device; they keep your screen oriented as you rotate it, enable mapping applications, tell you when you are low on power, etc. But it turns out that the data can being used off the phone as well. For example, if data from and accelerometer, gyroscope, and magnetometer data is reported off phone, the information can be used to locate a user *inside* a building, including what floor and what office—and thus whether the user has gone to the dermatologist's office in the medical building or the abortion clinic. So while a user might have shut off GPS data location from the device, data from on-device sensors could reveal where the user's destination. This is a not a theoretical concern; studies have shown that apps do collect accelerometer, gyroscope, and magnetometer data from users' devices.[5] How they use the data is not disclosed, but from patents, we do have some information about how companies might be using data from sensors.

Companies have obtained patents to:

- Use accelerometer information to determine whether two users have frequently been in close proximity on the same form of transport (e.g., a bus or the T) and aren't any longer, as a way to suggest a contact ("someone you may know");[6]

- Determine relationships between users in a crowd by whether they share network IDs;[7]

- Track a user, their interests, their social information, and their location within a store, in order to serve them timely ads depending on where they are and what they might be looking at, then tracking whether they bought a featured item.[8]

- Determine what user is doing in order to decide whether to deliver a message to them now—or wait until the person is more available.[9]

[4] For example, if there's lots of communications between the CEO, CFP, and corporate counsels of two companies, is that an indication of an intended merger? Communication patterns could reveal certain personal relationships, such as an extramarital affair.

[5] See, e.g., Andreas Claesson and Tor E. Bjorstad, Norwegian Consumer Council, "Out of Control: A Review of Data Sharing by Popular Mobile Apps," (2020), https://fil.forbrukerradet.no/wp-content/uploads/2020/01/mnemonic-security-test-report-v1.0.pdf at 46.

[6] B. Chen, "Systems and methods for utilizing wireless communications to suggest connections for a user," 2016, US Patent 9294991.

[7] B. Chen, "Systems and methods for utilizing wireless communications to suggest connections for a user," 2016, US Patent 9294991.

[8] J. D. Busch, "Systems and methods to attribute real-world visits of physical business locations by a user of a wireless device to targeted digital content or publicly displayed physical content previously viewable by the user," Jan. 28, 2020, US Patent 10546324.

[9] The determination of location and activity includes monitoring data from sensors measuring acoustic, temperature, humidity, accelerometer, gyroscope, altitude and more; see eBay, Methods and Systems for Providing Notifications Based on User Activity Data, July 24, 2017, U.S. Patent No. 2016/0037482 A1.

Note that none of this type of collection and use could reasonably be anticipated by the average user. Nor, short of not carrying a smartphone, could a user prevent such collection and use. A user is neither in a position to prevent the collection or use of communications metadata or device telemetry. This is why the minimization aspects of Massachusetts Data and Digital Privacy Act, which ensure that such data will be used *only for the purposes for which they were collected,* are so very important.

I would add an additional exception to Section 2's Duty of Loyalty, which would be to allow the use of such data for aggregate tracking in the case of publicly declared public health emergency, such as a hurricane—and then only for a very limited time period of, say, a maximum of a week. While such emergencies are less common in our state than in areas more prone to natural disasters, the exception is a useful one borne out of experiences elsewhere. It would also be a good model to include for states more prone to such acts of nature.

Do pass this bill. It is important for our privacy, our safety, and our security.

Thank you for your time and attention.