Susan Landau[1]
Testimony Before the Massachusetts Legislature
Joint Committee on Advanced Information Technology, the Internet and Cybersecurity
March 28, 2023

Thank you for the opportunity to offer testimony about providing statewide policy frameworks for protecting the Massachusetts public.

For more than thirty years, my research and scholarship has focused on the security and privacy of communications systems, largely on encryption policy and surveillance, but also on privacy risks. My work has often focused on public policy issues; in this vein, I have testified before the U.S. Congress, as well as having served on study committees of the National Academies of Science, Engineering, and Medicine, the Carnegie Endowment for International Peace, and other organizations.

I am currently 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. Previous to my time at Tufts University, I held positions as 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, Amherst 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 tell, I have spent much of my career in Massachusetts; at various times, I have called eastern and western Massachusetts home.

There are many important issues to discuss on the topic of this hearing; today I will focus on needed privacy protections for private citizens, an issue of important public safety and security, including national security. I want to begin by applauding this committee for its attention to this matter and for the development of the Massachusetts *Data Privacy Protection Act* (H. 83/S. 1743). Many people here today will say strong things about the importance of this bill; I want to draw your attention to an issue that has so far received little attention in public about private-sector collection of personal data that endangers us all. This is the collection and use of data that users are unaware of sharing from smartphone communications metadata and device and software telemetry.[2]

---

[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.

[2] Much of my testimony is derived from a forthcoming paper, Susan Landau and Patricia Vargas Leon, "Reversing Privacy Risks: Strict Limitations on the Use of Communications Metadata and Telemetry Information," to appear, Colorado Technology Law Journal, and Sarah Radway and Susan Landau, "SoK: Categorizing the Privacy Harms from Smartphone 'Non-Content' Data Collection and Use," preprint.

Smartphones have become an essential device for navigating modern life; they are needed for work calls and work meetings, for showing boarding passes and Covid vaccines, for reading email and responding to social media between meetings, and for sharing photos of one's children and grandchildren. But these remarkably versatile devices are also devices that leak data about our daily activities to ISPs, random WiFi networks as we traverse cities, train stations, and office buildings, apps, and websites. Much of this information is collected and aggregated, with fine-tuned portraits of us created and shared without our knowledge.

Let me start first with location information. You might feel anonymous as you traverse the city with your smartphone on—*but you are not.* The ubiquitous presence of cell towers and WiFi routers, which provide tremendous benefits in terms of connectivity and enabling user services, are terrific tracking devices. You might think that shutting off GPS location keeps your activities private, but that is not so. It takes only a few location points such as cell sites or WiFi routers to identify a user. Using just four spatio-temporal points, researchers in 2013 were able identify 95% of the individuals from a pool of 1.5 million.[3] What is particularly striking about this is that, unlike GPS data, the cell site location information and WiFi access points are data that users cannot prevent providing unless they shut off of their phones completely.

There are other sources of personal data as well, sources of which users have little awareness. When a user enters terms to Google or a mapping application, she knows she is providing that personal information. But when a user communicates via an encrypted Voice over IP (VoIP) call, she has no idea that the communications metadata leaks what language she is speaking—or even sometimes what she is saying. And when a user shuts off GPS collection so as to keep her destination private from applications, she doesn't know that other information—accelerometer, gyroscope, and magnetometer data, may provide information to apps about her location—including what office or room she is within a building. So while the GPS data she carefully shut off simply could have reported that the user had arrived at a set of medical offices, the data from on-device sensors could reveal her path within the building. It could reveal whether the user had gone to the oncologist's office or the abortion clinic.

The regulated telephone monopoly, AT&T collected and measured trunk traffic essentially from its beginning in order to determine how its services were working. It also recorded customer use of the telephone system for billing purposes. With the arrival of IP-based communications and smart phones, search collection and usage went into overdrive. The nature of IP based routing and delivery means that there is much richer data in Internet communications that have been in PSTN. When the world moved to cloud services, there was interest in collecting "telemetry" information: data about how the software was working.

As cellphones became smartphones, they acquired sensors, including accelerometers, gyroscopes, magnetometers, power sensors, proximity sensors, ambient noise sensors, and power sensors. These were useful for ensuring that the smartphones functioned properly and provided services, such as mapping applications. But their data also proved useful off device as well. U.S. and foreign industry has been patenting the use of communications metadata and sensor information for various purposes; examples include:

---

[3] Y.-A. De Montjoye, C. A. Hidalgo, M. Verleysen, and V. D. Blondel, "Unique in the crowd: The privacy bounds of human mobility," Scientific reports, vol. 3,no. 1, pp. 1–5, 2013.

- Using 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 longe, as a way to suggest a contact ("someone you may know");[4]
- Determining relationships between users in a crowd by whether they share network IDs;[5]
- Tracking 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.[6]

Some information can have high public benefit, e.g., location of mobile phones can help predict spread of dengue fever,[7] location of mobile phones plus understanding of social networks can help predict spread of HIV,[8] movement of people on public transportation can provide useful information for urban planners, etc. But other types of uses can be, per above, highly invasive.

Metadata and telemetry—information that smartphone users cannot control the collection of and cannot prevent the use of—can track movements of groups of people (a peaceful protest for example), the nature of relationships between people (whether their phones share networks, indicating proximity at various times of day), demographics, location, activity and behavior, user mental state and personality. And all of that is being shared without user knowledge.

It is for this reason that Massachusetts *Data Privacy Protection Act* (H. 83/S. 1743) and *An Act protecting reproductive health access, LGBTQ lives, religious liberty, and freedom of movement by banning the sale of cellphone location information* are so important (H.357/S.148).

Thank you.

[4] B. Chen, "Systems and methods for utilizing wireless communications to suggest connections for a user," 2016, US Patent 9,294,991.
[5] B. Chen, "Systems and methods for utilizing wireless communications to suggest connections for a user," 2016, US Patent 9,294,991.
[6] 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 10,546,324.
[7] A. Wesolowski, N. Eagle, A. M. Noor, R. W. Snow, and C. O. Buckee, "The impact of biases in mobile phone ownership on estimates of human mobility," *Journal of the Royal Society Interface*, vol. 10, no. 81, p. 20120986, 2013.
[8] F. Jing, Y. Ye, Y. Zhou, H. Zhou, Z. Xu, Y. Lu, X. Tao, S. Yang, W. Cheng, J. Tian et al., "Modelling the geographical spread of HIV among MSM in Guangdong, China: a metapopulation model considering the impact of pre-exposure prophylaxis," Philosophical Transactions of the Royal Society A, vol. 380, no. 2214, p. 20210126, 2022.