

Expert Report of
Jennifer King, Ph.D.

Public Redacted Version

IN THE SUPERIOR COURT OF THE STATE OF ARIZONA

IN AND FOR THE COUNTY OF MARICOPA

STATE OF ARIZONA, <i>ex rel.</i> MARK)	No. CV2020-006219
BRNOVICH, Attorney General,)	
)	
Plaintiff,)	
)	Assigned to the Hon. Timothy Thomason
v.)	
)	(COMPLEX CALENDAR)
GOOGLE LLC, A Delaware Limited Liability)	
Company,)	
)	
Defendant.)	
_____)	

Expert Report of Jennifer King, Ph.D.

May 4, 2022

TABLE OF CONTENTS

I. INTRODUCTION AND SUMMARY OF CONCLUSIONS..... 3

II. OVERVIEW OF QUALIFICATIONS 5

III. INFORMATION SCIENCE AND INFORMATION PRIVACY 6

IV. GOOGLE COLLECTS SUBSTANTIAL AMOUNTS OF LOCATION DATA THROUGH ANDROID DEVICES AND GOOGLE SERVICES..... 10

A. Industry Background..... 11

B. Google Collects Location Data By Design..... 15

V. MAKING LOCATION COLLECTION REAL: STUDIES SHOWING HOW MUCH DATA CAN BE COLLECTED 22

A. 2018 Schmidt Study of Android Location Collection 23

B. UC Berkeley RiseLab Posts by K. Shankari Related to Google, Internal Reaction At Google, and Subsequent AP Article..... 25

C. 2017 Quartz Investigation.....29

D. Professor Zuboff’s Study of Google Over Its History..... 29

E. 2019 New York Times Location Data Study..... 38

VI. HARMS FROM LOCATION DATA TRACKING..... 40

A. Data Collection Implicates Privacy Concerns 41

B. The Paradigm Shift Towards Always-On Location Collection Implicates Privacy Concerns Specifically 45

C. How Google’s Location Data Collection Harms Privacy 50

D. Location Data Collection Can Also Cause Financial Injuries to Consumers..... 55

E. Other Factors Affecting Harm..... 57

F. Tracking Harms Are Not Reasonably Avoidable By Consumers..... 59

VII. GOOGLE’S PROPOSED JUSTIFICATIONS DO NOT OUTWEIGH THESE HARMS 67

VIII. CONCLUSION..... 69

Appendix 1: Case-Related Documents Reviewed.....72

Exhibit A: Jennifer King, Ph.D. Resume, May 3, 2022

I. INTRODUCTION AND SUMMARY OF CONCLUSIONS

I was retained by counsel for the State of Arizona as an independent expert concerning Information Privacy and related issues that emerge in the context of collecting location data from smart phones and similar devices. I understand that the State of Arizona has accused Google of violating the Arizona Consumer Fraud Act through Google’s deceptive and unfair collection of users’ location data when they interact with Google’s products and services. I understand that the Arizona Consumer Fraud Act, like federal law and the laws of many other states, prohibits both “deceptive” and “unfair” acts and practices. I understand that Arizona law also provides for civil penalties for willful violations of the Consumer Fraud Act, and that the State has accused Google of acting willfully. I was specifically asked to consider whether and how the conduct alleged here relates to consumer harm, and to assist the factfinder considering that issue.

I have reviewed the State’s Complaint, and the November 16, 2021 Declaration of Dr. Seth Nielson, as well as other documents to understand some of the specific allegations leveled against Google in this case. A list of case-related documents I have reviewed is provided in the footnotes to this report; in addition, Appendix 1 at the end of this report provides a listing of case-related documents I reviewed, but the footnotes include further articles and websites that I reviewed and that constitute part of the facts and data I considered in forming my opinions. To assist the factfinder in deciding these issues, I was asked to apply my background in the field of Information Privacy and to consider whether (and, if so, how) Google’s conduct alleged here causes injury to consumers.

In this report, I also provide an overview of the above issues, reviewing what constitutes location data, why companies collect this data, and how it is collected using smartphones. I

review studies that examine how much data can be collected, and how individuals can be identified through even “anonymized” location data. In the report, I also discuss some of the harms caused by systematic location data collection, how these harms implicate privacy concerns, and why these harms are not reasonably avoided by consumers. I then explain why consumers have a privacy interest in their location data. More particularly, I address how Google’s conduct as outlined by the materials reviewed by me does, in fact, cause these harms. Finally, I address some of the justifications offered by Google in this case.

As I explained in more detail below, it is my opinion that the systematic collection, storage and exploitation of consumers’ personal location data as alleged by the State in this case causes various and significant harms to consumers, and that consumers cannot reasonably avoid those harms on their own. These harms include loss of privacy and loss of autonomy. These harms also include direct and indirect financial harms like price discrimination and advertising-based discrimination, including exclusion from some types of advertisements (ads) based on location-derived characteristics; the use of the consumer’s own data plan to transmit this location data to the servers collecting it; and the loss of the ability by consumers to potentially monetize this data themselves.

Further, the harms to consumers are further exacerbated because Google gives consumers the illusion of choice through settings and disclosures that are not only difficult to navigate but ultimately do not match their expectations. Google further uses location data beyond the context that a user would expect. In the end, Google also collects and stores more data and holds onto it longer than is actually necessary to provide services to consumers. The justifications and purported benefits offered by Google do not outweigh these concerns, especially given the serious allegations raised by the State.

II. OVERVIEW OF QUALIFICATIONS

I am the Privacy and Data Policy Fellow at the Stanford University Institute for Human-Centered Artificial Intelligence (HAI), where I research issues related to information privacy and artificial intelligence. I obtained my Ph.D. in Information Management and Systems (Information Science) from the University of California, Berkeley School of Information in 2018, with an emphasis in Human-Computer Interaction (HCI), information law and policy, and social computing. Prior to joining HAI in January 2021, I was the Director of Consumer Privacy at the Center for Internet and Society at Stanford Law School. Prior to obtaining my Ph.D. and working in the research field, I received a Master of Information Management and Systems (MIMS) degree in 2006, also from the U.C. Berkeley School of Information. I also worked for nearly a decade in the Internet software industry, as both a product manager and web producer, where my work encompassed a range of companies and specialties.

I am an internationally recognized information privacy scholar with approximately fifteen years' experience of empirical research, and I speak regularly at a wide range of academic, civil society, regulatory, and industry sponsored conferences and events, as well as to the media. My research has received multiple awards; my dissertation exploring the impact of power dynamics on individuals' decisions to disclose personal information was selected as the 2019 runner up for the iSchools' Conference Best Dissertation Award¹, and I have had multiple papers selected for the Future of Privacy Forum's "Privacy Papers for Policymakers" award. I co-authored one of the definitive surveys on consumer privacy in the past decade in 2009, resulting in two reports

¹ <https://ischools.org/Dissertation-Award-Past-Winners>

that have received hundreds of citations.² My research on privacy issues with smartphones³ was cited by the Federal Trade Commission in their 2013 report, “Mobile Privacy Disclosures: Building Trust Through Transparency,”⁴ and I was interviewed for a front-page story in *The New York Times* based on this work.⁵

Enclosed as Exhibit A is copy of my résumé, which also includes a list of any publications from the past 10 years, as well as a list of any cases where, in the past four years, I have given testimony as an expert at a hearing or trial.

I am being compensated for my work on this case at the rate of \$450/hour. My compensation is not contingent on the outcome of the case or the nature of my opinions.

III. INFORMATION SCIENCE AND INFORMATION PRIVACY

Information science is an interdisciplinary academic field that spans the social sciences, library science, as well as computer science. According to one definition, it is “the science and practice dealing with the effective collection, storage, retrieval, and use of information. It is concerned with recordable information and knowledge, and the technologies and related services that facilitate their management and use. More specifically, information science is a field of

² Hoofnagle, Chris Jay, King, Jennifer and Li, Su and Turow, Joseph, *How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies?* (April 14, 2010); and: Turow, Joseph and King, Jennifer and Hoofnagle, Chris Jay and Bleakley, Amy and Hennessy, Michael, *Americans Reject Tailored Advertising and Three Activities that Enable It* (September 29, 2009).

³ Jennifer King. *How Come I’m Allowing Strangers To Go Through My Phone? Smartphones and Privacy Expectations*. Workshop on Usable Privacy and Security for Mobile Devices (U-PriSM) at SOUPS, July 2012. Washington, D.C., USA.

⁴ <https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf>

⁵ https://www.nytimes.com/2013/10/06/technology/selling-secrets-of-phone-users-to-advertisers.html?_r=0

professional practice and scientific inquiry addressing the effective communication of information and information objects, particularly knowledge records, among humans in the context of social, organizational, and individual need for and use of information. The domain of information science is the transmission of the universe of human knowledge in recorded form, centering on manipulation (representation, organization, and retrieval) of information, rather than knowing information.”⁶ The field originated with the professionalization of librarianship, and several information schools today continue to offer degrees in library science. The official coalition of information science colleges and universities, the iSchools organization, counts 125 members⁷, including leading research universities such as: the University of California, Berkeley; University of Arizona; University of Michigan; University of Washington; and Carnegie Mellon University, among others.

Information privacy, also called data privacy or digital privacy, specifically refers to the use and governance of personal information, or “the right to have some control over how your personal information is collected and used.”⁸ As a field of study, this includes defining what constitutes “personal” information, understanding people’s expectations of privacy with respect to their personal information, how personal information is collected and used throughout society, the laws and policies that govern these uses, and the implications of all of these aspects on societies. As the world increasingly depends on digital data, questions of how to manage personal information are critical not only for the public sector but the private sector as well. Governments must collect and manage data about their citizens for many purposes, including providing benefits or facilitating education and public health. The collection of personal

⁶ Saracevic, T. (2009). Information science. In M. J. Bates (Ed.), *Encyclopedia of library and information sciences* (3rd ed.) (pp. 2570-2585). New York: Taylor and Francis.

⁷ <https://ischools.org/>

⁸ <https://iapp.org/about/what-is-privacy/>

information by private companies about consumers is one of the critical social issues of our times, as technology companies with vast data holdings are some of the wealthiest and most powerful companies to have ever existed, in large part because of the value of their data. And “[a]s the technology gets more sophisticated (indeed, invasive), so do the uses of data.”⁹

Given the complexity of these issues, even sophisticated companies employ specially-trained privacy experts to assist with a variety of issues including product design and review and also handling of events such as data breaches. In product design, privacy professionals often follow the methodology of “privacy by design,” a framework developed by a former privacy commissioner in Canada, Dr. Ann Cavoukian, which provides a set of principles by which to guide the development of technological systems and services.¹⁰ Other principles include The Fair Information Practice Principles (“FIPPs”), which include such principles as notice, choice, access, accuracy, data minimization, security, and accountability.¹¹ The IAPP has a similar listing of Fair Information Practice Principles.¹² Additionally, other academics such as Helen Nissenbaum and Alan Westin have also contributed to the literature for evaluating privacy interests, which I will discuss in more detail below.

As a scholar of information privacy, I take several approaches to studying the topic. My research is grounded in both qualitative methods (such as interview studies) and quantitative methods (such as surveys, survey experiments, data analysis), as well as methods used by human-computer researchers and practitioners for the study of computer interfaces, such as heuristic analyses, and various forms of user interface testing. Although I am not providing

⁹ <https://iapp.org/about/what-is-privacy/>

¹⁰ Dr. Ann Cavoukian, Privacy By Design - The Seven Foundational Principles. Jan. 2011. Available at: <https://iapp.org/resources/article/privacy-by-design-the-7-foundational-principles/>.

¹¹ See FTC Staff Report, Internet of Things: Privacy and Security in a Connected World, 34, 36 (Jan. 2015), <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>

¹² <https://iapp.org/resources/article/fair-information-practices/>

opinions on these issues in this case, a key area of my expertise focuses on how graphical user interfaces are designed in ways that promulgate deception, confusion, coercion, or manipulation, either through deliberate intent on the part of designers, or through poor design choices (commonly called “dark design patterns”). In addition, I also practice in the field of Human-Computer Interaction, or HCI, which is the study of how humans engage with computer interfaces. HCI is rooted in the field of human factors and ergonomics, which studies how humans interact with the physical world in order to improve the effectiveness, safety, and usability of specialized machines. Two principles emanate from the literature: first, humans have a universal desire for privacy, which extends to data about them; and second, privacy is an important democratic value and is essential for a free society. However, working with these two principles, my role is to understand what a specific population thinks of or needs from privacy.

Persons in this field who have been influential include theorists such as Helen Nissenbaum, Alan Westin, Sandra Petronio, and Irwin Altman, all of whom have articulated theories of privacy in digital, social, and legal contexts to explain humanity’s desire for this value. Helen Nissenbaum’s work, whose theory of contextual integrity is centered on *contextually appropriate flows of information*, posits that our expectations of privacy are context-dependent and influenced by social norms. For example, I have specific expectations of privacy in information that I disclose in one context (e.g., details about my health to my doctor) that are influenced by factors such as laws and professional practices, and I disclose assuming my doctor won’t violate those expectations, such as by posting my health information to a social media service, or selling it to a pharmaceutical corporation. Disclosing information in this context does not mean I’ve given up my expectations of privacy with regards to how my doctor handles that information or that my doctor can spy on me in any way he or she chooses beyond

the scope of my consent. I might also disclose the same information to a family member, again with specific expectations based on that context (i.e., that my spouse would keep the information confidential). Professor Shoshana Zuboff is another influential academic, whose research theorizes about the effects on society of mass surveillance and processing of personal data by companies, which she calls “surveillance capitalism.”¹³

For purposes of this report, I am applying my academic training and expertise, as well as my academic and professional experience, to assist the factfinder in understanding the harms (privacy and otherwise) from the collection, storage, and use of consumer location data from smartphones and, specifically, from the systematic tracking of location without consumer consent. I am also applying my training, expertise, and professional experience to help the factfinder understand the ability of consumers to avoid such collection (or lack thereof). Finally, I am applying my training, expertise, and professional experience to assist the factfinder in understanding whether the harms of systematic location tracking are outweighed by the benefits to consumers or competition. My analysis focuses on the population of U.S.-based smartphone users (including Arizona users) and the time period of the last approximately 14 years.

IV. GOOGLE COLLECTS SUBSTANTIAL AMOUNTS OF LOCATION DATA THROUGH ANDROID DEVICES AND GOOGLE SERVICES

In this section I provide some context for the opinions that follow, including a description of some of the allegations alleged here against Google. In addition to reviewing Nielson’s Declaration and the Complaint in this case, I also reviewed Professor Schmidt’s 2018 study

¹³ See, e.g., Shoshana Zuboff. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Public Affairs: 2019.

(discussed below), and a September 14, 2018 whitepaper prepared by Oracle, both addressing Google’s location collection practices. I also reviewed other sources discussed in the report and in the appendices, and I applied my own background and academic understanding of the issue of how location tracking works. I also previously conducted research in this area and published a paper in 2012 entitled “How Come I’m Allowing Strangers To Go Through My Phone? Smartphones and Privacy Expectations” that explored consumer privacy expectations with smartphones at that time in depth.¹⁴ I am also a co-author of a conference paper with colleagues from U.C. Berkeley that explored security issues on the Android mobile platform, specifically whether attribution mechanisms would help Android users understand when a third-party application was engaged in suspicious or harmful behavior that indicated a security risk.¹⁵ I also published an article in 2019 urging consumers to change their default settings on their smartphones to take more control over location collection, under the assumption that turning off location services on both Android and iOS platforms would curb the amount of tracking consumers experienced.¹⁶ This article was republished across hundreds of news sites around the world.

A. Industry Background

While digital devices using GPS to obtain location coordinates have existed since the late 1990s, it was the introduction of smartphones that made the widespread tracking of individuals’

¹⁴ Jennifer King. *How Come I’m Allowing Strangers To Go Through My Phone? Smartphones and Privacy Expectations*. Workshop on Usable Privacy and Security for Mobile Devices (U-PriSM) at SOUPS, July 2012. Washington, D.C., USA.

¹⁵ Christopher Thompson, Maritza Johnson, Serge Egelman, David Wagner, and Jennifer King. 2013. *When it's better to ask forgiveness than get permission: attribution mechanisms for smartphone resources*. In Proceedings of the Ninth Symposium on Usable Privacy and Security (SOUPS '13). Association for Computing Machinery, New York, NY, USA, Article 1, 1–14.

¹⁶ Jennifer King. “Change your phone settings so Apple, Google can’t track your movements.” *The Conversation*, January 14, 2019. <https://theconversation.com/change-your-phone-settings-so-apple-google-cant-track-your-movements-109059>

location possible. Given their near ubiquity today, it can be difficult to recall that smartphones have only existed for about fifteen years. Apple’s iOS platform launched in 2007, and Google’s Android in 2008.¹⁷ From the beginning, smartphones included many different sensors that traditional cell phones did not, including a GPS receiver. In this section, I discuss how this data is collected, and note that the widespread collection of location data is enabled by design, both by smartphone operating systems as well as the system of user interfaces and permissions designed to enable consent.

As background, traditional mobile phones (non-smartphones) tracked subscriber location via the provider’s network of cell towers, which registered each time a phone contacted a specific tower. Providers kept records of these “pings,” which could roughly identify where a phone was in a specific geographic area. However, this data was held by mobile providers (e.g., AT&T, Verizon, etc.) and while mobile providers have (somewhat controversially) sold cell service location data, its commercialization was not as widespread as smartphone location data is today, likely in part because potential customers (e.g., third party application (app) developers) had to purchase the data directly from each provider.

Smartphones made new forms of location data available not only to the operating system (e.g., Android), but also to app developers that requested location data for their programs. Like the traditional mobile phones that preceded them, smartphones can track user location via a provider’s cell towers, registering each time a phone contacts a provider’s tower. But unlike cell service data, Google’s location data derived from a smartphone’s GPS and other sensors is free and available, immediately, in real time.

¹⁷ “T-Mobile officially announces the G1 Android phone.” Tech Crunch, September 23, 2008. <https://techcrunch.com/2008/09/23/t-mobile-officially-announces-the-g1-android-phone/>.

According to survey research by the Pew Research Center, 97%¹⁸ of U.S. adults today use a smartphone. Furthermore, we all spend a great deal of time using our smartphones; one mobile analytics firm estimates that individuals spend an average of 4.8 hours per day on mobile devices.¹⁹ At the same time, chances are your phone has some, if not all, of its user-controllable sensors enabled: Wi-Fi for connecting to local Wi-Fi networks for internet access, Bluetooth for connecting to wireless devices (such as headphones or speakers), and location services, to receive its geographic location (“geolocation”) from global positioning satellites (GPS) orbiting the Earth.

Today, various sensors (like Wi-Fi, Bluetooth and others), not just your smartphone’s GPS receiver, work in various ways to plot the geolocation of your phone on the planet as precisely as possible. And this can happen not just when you are actively using a mobile app or engaged in some other activity on your phone, but also in the “background,” even when you’re not using it. Hour by hour, day by day, versions of that location data are being collected by many different actors—by the phone’s operating system (such as Google’s Android), directly by many of the apps on your phone, and also indirectly through many of your mobile apps if the creators used a software development kit (SDK) that allows them to monetize (to earn money from) a user’s usage of their app.

Through various application programmer interfaces (APIs²⁰) created for Android, Google presently offers two forms of location access to app developers: “approximate” (coarse)

¹⁸ <https://www.pewresearch.org/internet/fact-sheet/mobile/>

¹⁹ <https://www.data.ai/en/insights/market-data/state-of-mobile-2022/>

²⁰ APIs are interfaces that make it easier for apps to communicate with other apps and services. They lighten developers’ burden to design processes from scratch. Google provides various APIs that enable the use and collection of location data. Many of these are included in Google Play Services, a background service and API package introduced in 2012 that today is installed on almost all Android devices. While Android is an open-source operating system, meaning it is

and “precise” (fine).²¹ According to the documentation, the fine location permission allows an app to access “as precise a location as possible from the available location providers, including the Global Positioning System (GPS) as well as WiFi and mobile cell data.” The strength of a device’s WiFi or Bluetooth connection can indicate its relative proximity to hotspots or access points. Proprietary databases can assign those hotspots and access points known location coordinates, thereby permitting these signals to be used to derive location. According to Google’s current developer-facing documentation, estimates for fine geolocation range from 10 feet to 160 feet in accuracy.²² According to the same Google documentation, coarse location is accurate within a range of 1.2 square miles.

I understand (including from the Complaint and from Dr. Nielson’s declaration) that Google collects location data through the Android operating system itself,²³ as well as through its own mobile applications and services developed for Android devices, termed Google Mobile Services (GMS). These apps, including Google Chrome, Search, and Maps (among others), can both access and collect location information. While device manufacturers can decide whether to install GMS, I understand that the vast majority of Android phones sold in the United States have Google’s version (or the GMS version) of the operating system since they cannot offer many of the core Google functions without it.²⁴ Because all (or nearly all) Android users sign into their phones with a Google account, Google is able to associate location data with one’s Google account independently of one’s use of any Google apps.²⁵

based on freely available and modifiable source code, Google APIs are proprietary. Developers cannot modify what data the Maps API, for instance, collects, with what frequency, or how.

²¹ <https://developers.google.com/maps/documentation/android-sdk/location>

²² <https://developer.android.com/training/location/permissions#accuracy>

²³ Nielson 11/16/2021 ¶¶ 41-44.

²⁴ Nielson 11/16/2021 ¶¶ 41-44.

²⁵ Though it may be technically possible to use some Android phones without either a Google Account or using Google’s software, it is challenging to do so and requires the user to give up

In many cases, Google collects location data directly from services running on the smartphone’s operating system that are built into Android and that users cannot control or refuse. One such involuntary service is a “network sync system” that enables real-time messaging.²⁶ This service requires Android devices and servers to send pings, or “heartbeats,” to each other, maintaining server connectivity that enables real-time messaging. These heartbeats contain a device’s IP address, which Google, as discussed below, uses to calculate device location.

Further, as the network location provider,²⁷ Google can also collect location data from Android devices through Google Location Services (GLS).²⁸ This service combines GPS information with location information from various other sensors to more accurately calculate the position of a device.²⁹ When GLS is enabled on a device, Google periodically collects location data from the device to continue improving location accuracy.

B. Google Collects Location Data By Design

Google developed a number of different products and services that it uses to collect location data. Some of those are discussed in Dr. Nielson’s declaration.

much of the functionality and services. A few articles that discuss this option explain that the user would have to say “goodbye” not only to things like Android apps, but also social networks, music streaming services, popular games, most navigation tools, cloud storage providers, video stream sites, and many productivity tools. The user may also experience slower updates and resulting security risks that do not get patched. Those who suggest this option are precisely trying to avoid Google because “Google Has Gotten Out of Hand,” and they want to increase privacy. See: <https://www.makeuseof.com/tag/using-android-without-google/>, and <https://www.tomsguide.com/news/i-used-android-without-google-here-are-the-pros-and-cons> for a discussion of this topic.

²⁶ Described in Google’s letter to Senators Markey/Blumenthal:

<https://www.acc.gov.au/system/files/Oracle-Submission-2-%28September-2018%29.pdf>

²⁷ A network location provider derives your position from cell tower and WiFi access points.

²⁸ Also known as Google Location Accuracy.

²⁹ <https://policies.google.com/technologies/location-data?hl=en-US>

For example, Google acquired Android in 2005, which at the time was a relatively unknown startup focused on “software for mobile phones.”³⁰ In 2007, Google acquired an online ad company called DoubleClick for \$3.1 billion, which gave Google a large network of advertisers and Web publishers.³¹ As noted above, the first mobile device on the Android platform was released in 2008, and Google introduced the GMS and Google Play aspect of the platform in 2012. Dr. Nielson’s Declaration explains how the Android operating system in general, as well as the pre-loaded apps and Google account settings work together to collect location data.³²

Aside from the Android operating system, Google has proprietary technologies that make it able to collect and infer location in ways that are particularly precise and far-ranging. For example, in his Declaration dated November 16, 2021, Dr. Seth Nielson discusses Google’s proprietary IPGeo and [REDACTED] services. I understand Google has improved and refined these services over time, but Google’s planning for these services dates back more than a decade. For example, IPGeo is addressed in an internal Google presentation from 2009 entitled, Predicting user location from IP-Address, How hard can it be?”³³ According to the presentation, “IPGeo’s Mission” is “To predict users’ locations from their IP addresses by improving ways of exploiting available data, and to provide this knowledge to all Google products.”³⁴ Google’s internal “Confidentiality Notice” on the presentation states: “You have no idea how incredibly confidential this one is. My my, is this confidential. I kid you not. Imagine an article titled “Google knows where you live, because it spies on you” in the NYT. You’ve been warned.”³⁵

³⁰ <https://www.engadget.com/2005-08-17-google-buys-cellphone-software-company.html>

³¹ <https://www.cnet.com/tech/tech-industry/google-buys-ad-firm-doubleclick-for-3-1-billion/>

³² Nielson 11/16/2021 Decl. ¶98.

³³ GOOG-GLAZ-00222226.

³⁴ GOOG-GLAZ-00222226 at 27.

³⁵ GOOG-GLAZ-00222226 at 28.

As discussed below, this technology is specific to Google and only certain other companies, and facilitates systematic collection of location data. I understand that Google determines a user’s location through an IP address using these services.³⁶ I understand that the IPGeo service uses signals such as [REDACTED] to improve the location output. In this case, the State is alleging that Google tracks users regardless of their settings using IPGeo and [REDACTED], and that those proprietary databases are built using “users” and “reporters.”³⁷ Users who report their location are essentially co-opted by Google to determine the location of nearby users who have not reported their location.³⁸ Further, despite the various setting, there is no “opt-out” and there is nothing users can do to prevent Google from doing this.³⁹ Dr. Nielson explains that “just about any transaction with Google...becomes an opportunity for Google to collect, store, and exploit the users’ location information” because [REDACTED] is ‘independent of settings,’” and Google uses this information to serve ads.⁴⁰

Dr. Nielson also discusses a variety of settings on Android devices and in Google accounts that are used to collect location information, including Location History (“LH”), Web & App Activity (“WAA”), Device Location and others.⁴¹ The State’s Complaint points to Google’s internal document suggesting Google has long recognized that these settings are not well-understood by users.⁴² For example, an internal Google presentation dated October 2014 entitled “Simplifying Location History Settings (on Android)” explains the “Most users don’t understand difference between location reporting and location history.”⁴³ An email from August

³⁶ Nielson 11/16/2021 Decl. ¶98.

³⁷ Nielson 11/16/2021 Decl. ¶110.

³⁸ Nielson 11/16/2021 Decl. ¶109.

³⁹ Nielson 11/16/2021 Decl. ¶¶104-05, 116.

⁴⁰ Nielson 11/16/2021 Decl. ¶¶ 119-121.

⁴¹ Nielson 11/16/2021 Decl. ¶¶1 54-80.

⁴² Compl. pgs. 12-14.

⁴³ GOOG-GLAZ-00002914 at 2916.

2016 discusses “understanding the smörgåsbord of consents.”⁴⁴ The Complaint (at paragraphs 44-49, 60-69) quotes multiple internal documents where Google employees express their own concerns and display their own confusion by the settings. The confusion between some of these settings—including the fact that Google continues to collect user “location history” through WAA even when a setting called “Location History” is off—was the focus on an August 2018 AP Article discussed below.

In January 2017, Google engineers created a document titled “go/ul2017.”⁴⁵ That document states in part: “On this page below is the high-level map of the User Location landscape at Google in 2017. Our (already vast) landscape has evolved some new grey areas and ambiguities wrt. data collection, consent, transparency+control, and use. We collect User Location via so many channels that even Google engineers and PMs don’t fully comprehend it, let alone our 1B+ regular users across Android, Search, Maps, and many other Google products.” The document, under the heading “Context & Motivation,” later states: “It’s 2017 and the world is more comfortable than ever with sharing vast amounts of personal information with 3rd parties like Google and Facebook - and trusting them to do good, responsible things with it. At Google (and the broader Alphabet), *one of the most sensitive and vast personal signals that we collect from users is User Location.*”⁴⁶ David Monsees, a Google product manager, agreed in testimony before the Federal Court of Australia in *Australian Competition and Consumer Commission v. Google*, 2021 FCA 367 (NSD 1760 of 2019), that the location data generated by Google’s Web

⁴⁴ GOOG-GLAZ-00002914 at 2916.

⁴⁵ GOOG-GLAZ-00317865 at p. 1

⁴⁶ GOOG-GLAZ-00317865 at p. 4 (emphasis added).

and App Activity account-level setting is used to geo-target ads, and later agreed that location is “one of the most sensitive and vast personal signals we collect from users.”⁴⁷

The Complaint (at paragraphs 79-86) also alleges that Google shares location with apps that users explicitly forbid from using location. Again, the Complaint catalogues example of internal documents and emails suggesting that Google has known of these issues for years without addressing them. The Complaint (at paragraph 84) cites emails showing that [REDACTED]. Dr. Nielson also explains that Google’s Android operating system enables apps to obtain a user’s location even when a user denies those apps permission.⁴⁸

Google also collects and aggregates multiple signals, which are then made available to *hundreds* of internal Google apps and services. Dr. Nielson also explains that all of these various signals are aggregated by a central service called [REDACTED], which is “‘marketed’ within Google as the service to use if the app should change behavior based on location.”⁴⁹ Besides Ads, the location estimated by [REDACTED] is used “by 250+ clients at Google.”⁵⁰

The State’s Complaint (at paragraph 88) also discusses a policy at Google called “off means course.” Dr. Nielson explains that until around May 2019, [REDACTED] would return the most precise location it could.”⁵¹ At that point, Google implemented “off means course,” meaning that when a user turns “off” the “Location Master” on their device, Google interprets that as meaning

⁴⁷ GOOG-GLAZ-00299120, at 169; see also *ibid.* at 137 (admitting that Web and App Activity tracks user location for ads service).

⁴⁸ Nielson 11/16/2021 Decl. ¶32.

⁴⁹ Nielson 11/16/2021 Decl. ¶¶123, 129.

⁵⁰ Nielson 11/16/2021 Decl. ¶128.

⁵¹ Nielson 11/16/2021 Decl. ¶130.

Google should still infer a coarsened location. “Since that time, [REDACTED] returns a ‘course’ location to queries that do not already know the current location.”⁵²

The Complaint also alleges other conduct. For example, at paragraph 93, the Complaint alleges (with citations and quotations from Google’s internal documents and testimony) that “Google infers a user’s extremely sensitive home and work locations without consent,” including “when a user turns off Location History” and “when a user turns off *all* of a device’s location-related settings.” The State alleges in paragraph 94 (with similar support) that that [REDACTED] [REDACTED] In the Complaint (at paragraphs 129-131), the State also accuses Google of misleading and deceiving users regarding its deletion of their location information. Further, in paragraph 131 of the Complaint, the State points alleges: “what is worse is that Google’s user-facing interface displays data being deleted immediately,” but the opposite is true.

As explained above, this systematic collection of users’ location data is no accident. It happens by design. Geolocation tracking has been a core feature in smartphones since they were first sold in the late 2000s, and a surprising number of companies, including Google, can access your geolocation. Google in particular has focused on developing comprehensive and proprietary location tracking systems, leveraging all of its various services—including the Android operating system, GMS, Google Accounts, Maps, Chrome, IPGeo, [REDACTED] and others—to collect, aggregate and store location data, which is then made available to hundreds of Google clients. If a company’s conduct is deceptive or unfair, then it is regulated by the U.S. Federal Trade Commission through the FTC Act and state consumer protection laws.⁵³ Outside of

⁵² Nielson 11/16/2021 Decl. ¶130.

⁵³ Statement of Acting Director of FTC Bureau of Consumer Protection Daniel Kaufman: “Many of the dark patterns discussed today already are illegal under Section 5 of the FTC Act and state laws prohibiting deceptive and unfair practices, as well as Under the Restoring Online Shoppers’

consumer protection laws that prohibit deceptive and unfair conduct, however, no federal law presently exists in the U.S. that otherwise directly limits how much location data companies collect from you, how long they can keep it, how they use it, and whether they can elect to share it or sell it with others.⁵⁴ This is important for understanding what data-collection an informed user would consent to, as well as to the harms from the systematic collection of personal data.

In addition, location data is one type of personal data that Google collects that assists with inferring valuable things about a particular consumer's behavior and preferences. Other types of personal data include basic personal information like name, age, sex or gender, search terms, and browsing history, to name a few. Moreover, artificial intelligence (e.g., machine learning) can infer things about consumers based on connections between what may appear to be unrelated data points.⁵⁵ Thus, while the focus of this report is location data, that data does not exist in a vacuum but can be combined with other data and advanced processing to infer even more information about consumers.⁵⁶ Technology companies have the ability to collect and store vast amounts of data indefinitely, meaning that even minor interactions with an app or a service can be memorialized effectively forever. For example, until fairly recently, Google kept data

Confidence Act. And the FTC, along with its state and international partners, have been and will continue to be active in investigating and bringing suit to stop these unlawful practices.”

(4/29/2021), page 84 available at

https://www.ftc.gov/system/files/documents/public_events/1586943/ftc_darkpatterns_workshop_transcript.pdf

⁵⁴ Notably, this is changing as more U.S. states adopt their own specific data privacy laws.

⁵⁵ See generally: Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money And Information* (2015); Eric Horvitz and Deirdre Mulligan. “Data, Privacy, and the Greater Good.” *Science*, 17 Jul 2015 • Vol 349, Issue 6245 • pp. 253-255 • DOI:

10.1126/science.aac4520; Udacity.com. “Machine Learning for Big Data.” August 14, 2020.

<https://www.udacity.com/blog/2020/08/machine-learning-for-big-data.html>.

⁵⁶ See generally: Scott Thurm and Yukari Iwatani Kane. “Your Apps Are Watching You.” *The Wall Street Journal*, Dec. 18, 2010.

<https://www.wsj.com/articles/SB10001424052748704368004576027751867039730#ixzz18WF>

HX4pP; Julia Angwin And Jennifer Valentino-DeVries. “Apple, Google Collect User Data.” *The Wall Street Journal*, April 22, 2011.

<https://www.wsj.com/articles/SB10001424052748703983704576277101723453610>.

such as their users' location data and search terms forever, by default.⁵⁷ As part of my dissertation research, in 2016-2017 I interviewed twenty participants about their experiences with online search services; nineteen of the twenty participants were Google users. Some of those interviewees examined their Google search histories as part of our discussions (not all were aware that their search history was logged) and were surprised to find an in-depth accounting of every single search query they had entered into Google's search engine while they were logged into their accounts, in some instances reaching back a decade or more.⁵⁸ None had anticipated that their search histories could exist a decade after they entered a query into Google's search box, and nor did they anticipate that that data could be aggregated, used to build profiles of their behavior, and draw inferences about them, including in combination with other data collected across Google's products and services.

In sum, Google's systematic collection of location data combined with its other data and processing abilities thus poses specific privacy harms on a scale that few other companies can operate.

V. MAKING LOCATION COLLECTION REAL: STUDIES SHOWING HOW MUCH DATA CAN BE COLLECTED

The privacy issues and harms associated with location data collection can feel very abstract. After all, millions upon millions of people use smartphones. Why would your location data be of particular interest to anyone? Why would you stand out in the crowd? And what if you feel as if you have nothing to hide? Before answering those questions in this report, consider that

⁵⁷ <https://blog.google/technology/safety-security/keeping-private-information-private/>

⁵⁸ King, J. (2018). Privacy, Disclosure, and Social Exchange Theory. UC Berkeley. ProQuest ID: King_berkeley_0028E_17901. Merritt ID: ark:/13030/m5t77dzd. Retrieved from <https://escholarship.org/uc/item/5hw5w5c1>.

while it is true that your data might be collected, stored, and aggregated with millions of others’ data, it is important to understand the depth and precision with which location data can reveal the details of one’s daily life. Further, location data can uniquely identify you, even if the data is ‘anonymized.’ That is because the vast majority of us consistently return to the same places day after day: home, work, and/or school. By closely examining that data, it becomes possible to pick out and uniquely identify individuals even in very large datasets.⁵⁹

A. 2018 Schmidt Study of Android Location Collection

In 2018, Douglas Schmidt, a computer science professor at Vanderbilt University, published a research study surveying Google’s data collection practices across mobile, laptop, and desktop devices.⁶⁰ The study explored, among other things, a “day in the life” of an Android phone user, comparing the data mining that took place on Android and iPhone devices.

Schmidt’s research includes two key takeaways. First, that Google collects a wide array of data passively, via platforms (Android), applications, publisher tools, and advertising tools. Passive collection takes place in the background, often without users’ awareness. An idle Android phone, for instance, makes close to 40 requests per hour to Google’s servers, 35% of which communicate location data.⁶¹ Advertisers and publishers use Google’s fine-tuned understanding of user behavior to monetize a hyper-specific target audience.⁶² Google offers a

⁵⁹ See generally Rocher, L., Hendrickx, J.M. & de Montjoye, YA. “Estimating the success of re-identifications in incomplete datasets using generative models.” *Nat Commun* 10, 3069 (2019); Hui Zang and Jean Bolot. 2011. “Anonymization of location data does not work: a large-scale measurement study.” In *Proceedings of the 17th Annual International Conference on Mobile Computing and Networking (MobiCom ’11)*. Association for Computing Machinery, New York, NY, USA, 145–156.

⁶⁰ Douglas C. Schmidt, *Google Data Collection* (2018).

⁶¹ *Ibid.*, 14.

⁶² *Ibid.*, 15.

full suite of advertising tools that are used by millions of websites and advertisers to better cater to consumers.⁶³

Second, users lack straightforward control over the wide array of data that Google actively collects. Active collection occurs when users are using a service: e.g., when they sign into Google services or accounts, check-in to locations, download apps, or make various search requests. Schmidt finds this control nominal, often buried in long and confusing lists of settings that interact with each other in confounding ways. For example, the study describes how Android can collect location data via Wi-Fi scanning, a tool that scans for local geo-tagged Wi-Fi networks to improve location accuracy, even when users turn off their universal Wi-Fi setting.⁶⁴ Passive data collection also increases as user activity on their device increases.⁶⁵

While Google has released technical and policy updates over time related to user privacy across devices and products,⁶⁶ their business model today remains largely the same as what Schmidt's study suggested in 2018: collecting, using, and selling access to increasingly specific user behavior information, including location data. The 2018 Schmidt study informs the applicability of my opinions about privacy and other harms from location tracking to Google's conduct that underlies this case.

⁶³ Ibid., 15.

⁶⁴ Ibid., 12.

⁶⁵ Ibid., 3.

⁶⁶ In 2020, for example, Google began automatically deleting users' location history after 18 months.

<https://blog.google/technology/safety-security/keeping-private-information-private/>

B. UC Berkeley RiseLab Posts by K. Shankari Related to Google, Internal Reaction At Google, and Subsequent AP Article

In May and June 2018, a researcher at UC Berkeley published two blog posts by the RiseLab at UC Berkeley.⁶⁷ The RiseLab is a lab created by UC Berkeley computer science division to investigate “the next chapter in the ongoing story of data-intensive systems at Berkeley; a proactive step to move beyond Big Data analytics into a more immersive world.”⁶⁸ The RiseLab’s research agenda focuses on the intersection of ubiquitous sensor technology, artificial intelligence, and information security.

The May 2018 blog post is titled, “The Right to not be Tracked: a Spotlight on Google Maps and Android Location Tracking.”⁶⁹ The primary question addressed by this publication from Kalyanaraman Shankari seeks to answer the question of how did Google know that she visited Kohl’s department store and prompt her to “rate her visit” to the store. She raised the question of user consent where there is a blurring of the boundaries between the phone operating system and proprietary services. This initial publication from Shankari didn’t yet reach the conclusion that Google tracks user location no matter what.

Shankari followed up her May 2018 with a second post in June 2018. This article is titled “The Right to not be Tracked II: in which I turn off the location permission for Google, but it tracks me anyway.”⁷⁰ Shankari talks about the Google Now app, which is a “virtual assistant that is intended to provide context-sensitive helpful information to users. It is closed source, pre-

⁶⁷ <https://rise.cs.berkeley.edu/blog/the-right-to-not-be-tracked-a-spotlight-on-google-maps-and-android-location-tracking/>
<https://rise.cs.berkeley.edu/blog/the-right-to-not-be-tracked-ii-in-which-i-turn-off-the-location-permission-for-google-but-it-tracks-me-anyway/>

⁶⁸ <https://rise.cs.berkeley.edu/>

⁶⁹ <https://rise.cs.berkeley.edu/blog/the-right-to-not-be-tracked-a-spotlight-on-google-maps-and-android-location-tracking/>

⁷⁰ <https://rise.cs.berkeley.edu/blog/the-right-to-not-be-tracked-ii-in-which-i-turn-off-the-location-permission-for-google-but-it-tracks-me-anyway/>

installed, and it cannot be uninstalled or disabled.” Shankari was able to note that Google was tracking movements but did not come to a definitive conclusion as to how it did this. I find the Shankari publications to be reliable statements of tracking that she observed in the May and June 2018 time period.

An internal Google email picks up on the Shankari blog posts and is extremely telling and important for this report because it shows the “shock[]” one experiences from the type of location tracking at issue.⁷¹ This is an email chain between a Google employee named Blake Lemoine and Vint Cerf. Blake Lemoine identified himself as an engineer on the Google Now quality team, a virtual personal assistant program. Dr. Vint Cerf is an internet pioneer and one of the developers of TCP/IP—even known as one of the “fathers of the internet.”⁷² He lists his title at Google as VP, Chief Internet Evangelist and has been at the company since 2005.⁷³ Mr. Lemoine writes to Dr. Cerf regarding the Shankari articles. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] location information derived from IP addresses is an inescapable part of the internet so we don’t need users’ permission to use it. [REDACTED] I believe that the level

⁷¹ GOOG-GLAZ-00315032 at 34.

⁷² https://en.wikipedia.org/wiki/Vint_Cerf

⁷³ <https://www.linkedin.com/in/vint-cerf-869259180/>

of accuracy of our IP Geo system is far beyond anything achievable based solely on the location information inherent in IP addresses. I believe that we are deceiving users by telling them they can turn off location and then spending millions of dollars to infer their location through other means. [REDACTED] I feel like we're lying to our users by giving them a permission setting that we then find a way around."⁷⁴

Dr. Cerf responds first that Lemoine “makes a good point that we appear to be tracking even when users have turned off what they think and what we imply are tracking mechanisms.”⁷⁵ He then continues that he was “shocked that Google had created a timeline of date, hour, location, and route for 18 months of [his] movements, including maps and street addresses. [He] only discovered this because someone had suggested [he] should look at the Google Maps Timeline.”⁷⁶

These posts by Shankari also led a few months later to the publication of an article by the Associated Press titled “Google Tracks Your Movements, Like it or Not.”⁷⁷ The AP article found that “Google stores a snapshot of where you are when you merely open its Maps app. Automatic daily weather updates on Android phones pinpoint roughly where you are. And some searches that have nothing to do with location, like ‘chocolate chip cookies,’ or ‘kids science kits,’ pinpoint your precise latitude and longitude — accurate to the square foot — and save it to your Google account.” The AP Article further reports that a researcher from the lab of Jonathan Mayer, a Princeton computer scientist and former chief technologist for the Federal Communications Commission’s enforcement bureau, confirmed the AP’s findings on multiple Android devices; the AP conducted its own tests on several iPhones that found the same

⁷⁴ GOOG-GLAZ-00315032 at 34.

⁷⁵ GOOG-GLAZ-00315032 at 33.

⁷⁶ Ibid.

⁷⁷ <https://apnews.com/article/north-america-science-technology-business-ap-top-news-828aefab64d4411bac257a07c1af0ecb>

behavior. I find the AP article to be a reliable description of certain of Google’s location tracking practices. I find this article, and the statements therein, reliable including because it independently had researchers at Princeton University reproduce the results obtained by Shankari. I used both the AP article and Shankari’s posts in part for the basis of the article I wrote for *The Conversation* in 2019.⁷⁸

I understand from a document produced in this case that Google held an “Oh Shit” meeting regarding the AP article shortly after its publication.⁷⁹ Google’s Communications and Public Affairs Director emailed regarding this meeting that “[b]oth comms and policy are looking for an update on where we are in terms of fixing ‘location history’ fixes [sic] and having one single place to turn off instead of 3.”⁸⁰ Very senior Google employees (including CEO Sundar Pichai) were involved in crafting Google’s response to the AP Article.⁸¹ CEO Pichai called a “code yellow” meeting to get updates on the issues discussed in the AP Article from Google’s Senior Vice President of Geo and Maps, Jen Fitzpatrick.⁸²

C. 2017 Quartz Investigation

Half a year before the Shankari blog posts, the website Quartz published a study titled, “Google collects Android users’ locations even when location services are disabled.”⁸³ This article by Keith Collins, described the practice of Android sending cell tower IDs back to Google. Google claimed this was to improve message delivery. The article reported: “It is not clear how cell-tower addresses, transmitted as a data string that identifies a specific cell tower, could have been used to improve message delivery. But the privacy implications of the covert

⁷⁸ King, *supra* note 16.

⁷⁹ GOOG-GLAZ-00001521, 523.

⁸⁰ *Ibid.*

⁸¹ *See e.g.* GOOG-GLAZ-00001371, 373.

⁸² *Ibid.*

⁸³ <https://qz.com/1131515/google-collects-android-users-locations-even-when-location-services-are-disabled/>

location-sharing practice are plain. While information about a single cell tower can only offer an approximation of where a mobile device actually is, multiple towers can be used to triangulate its location to within about a quarter-mile radius, or to a more exact pinpoint in urban areas, where cell towers are closer together.” I find the results of this Quartz report reliable, including because Google confirmed them, as reported in the article.

D. Professor Zuboff’s Study of Google Over Its History

Professor Emerita Shoshana Zuboff of Harvard Business School wrote a watershed book published in 2019 titled *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*.⁸⁴ This book has been widely reviewed and praised, and I consider it reliable.

Professor Zuboff charts the development of what she calls “surveillance capitalism,” which encompasses a broader movement of businesses towards the practices of data-intensive collection practices than just Google’s actions in this area. But as to Google specifically, Professor Zuboff claims Google invented and perfected the practice.⁸⁵ Surveillance capitalism involves (1) collecting human experience; (2) translating it into behavioral data; (3) fabricating the data into prediction products that anticipate what you will do now, soon, and later using machine intelligence; (4) monetizing the data; and, eventually, (5) trading the data in “behavioral futures markets”—new markets she predicts will arise for trading in data.⁸⁶ She claims a 2014 ruling in the EU’s Court of Justice recognizing a “right to be forgotten” on Google Search was an inflection point after which democracy began to fight back against surveillance capitalism.⁸⁷

⁸⁴ Zuboff, *supra* note 13.

⁸⁵ *Ibid.*, p. 9 and p. 63.

⁸⁶ *Ibid.*, p. 8.

⁸⁷ *Ibid.*, p. 59.

She describes Google as a secretive company: “a 2016 lawsuit against the company by a product manager alleged an internal spying program in which employees are expected to identify coworkers who violate the firm’s confidentiality agreement: a broad prohibition against divulging anything about the company to anyone”.⁸⁸ She claims Hal Varian, the company chief economist and employee since 2002,⁸⁹ is the best source for insight into the majority of Google’s practices.⁹⁰ She also notes that Google became more secretive upon understanding the power of the data it was collecting—former CEO Eric Schmidt instituted what he called the “hiding strategy” discouraging employees from speaking about Google’s practices.⁹¹

Professor Zuboff argues that Google’s claim that it “does not sell personal data” is misleading because it does sell the predictions that only it can fabricate from its collection of behavioral information.⁹² Google’s acquisition of YouTube makes more sense in light of the opportunity for future behavioral data collection it represented.⁹³ Experts say our data is not de-identified from our personal selves, as tech companies claim. Research into reidentification techniques has demonstrated that individuals can be fully identified to the trove of data they produce using as few as three items of information culled from the public record (birth date, zip code, and sex).⁹⁴

Google Location Tracking. Professor Zuboff discusses Google’s location practices. When Larry Page was asked “What is Google?” in 2001, he posited, “If we did have a category, it would be *personal information*...The places you’ve seen. Communications...Sensors are really

⁸⁸ Ibid., pg. 64

⁸⁹ <https://people.ischool.berkeley.edu/~hal/>. Hal Varian is the former dean of the department where I received my master’s and doctoral degrees at U.C. Berkeley.

⁹⁰ Zuboff, *supra* note 13, pp. 64-65.

⁹¹ Ibid., pp. 88-89.

⁹² Ibid., p. 96.

⁹³ Ibid., p. 103.

⁹⁴ Ibid., pg. 245.

cheap...Storage is cheap. Cameras are cheap...Everything you've ever heard or seen or experienced will become searchable. Your whole life will be searchable".⁹⁵ In 2004, Google acquired Keyhole, a satellite mapping company – it became the backbone for Google Earth, Google Maps, and the controversial Street View project.⁹⁶

Professor Zuboff concludes that many smartphone apps “demand access to your location even when it's not necessary for the service they provide, simply because the answer to this question is so lucrative. Location data can be extracted from ‘geotags’ created when your smartphone automatically imbeds your identity and location in photos and videos. Retailers use ‘geofencing’ to demarcate a geographical area and send alerts to smartphones within those parameters”.⁹⁷

Professor Zuboff discusses that “Google represents the vanguard of location-based tracking. A 2016 affidavit...made plain why Google location data are unparalleled: ‘Google collects and retains location data from Android-enabled mobile devices. Google collects this data whenever one of their services is activated and/or whenever there is an event on the mobile device such as a phone call, text messages, internet access, or email access.’”⁹⁸ “The officials on the case requested location information from Google because it offers far more detail than even the phone companies can provide. The location system in Android combine cell-tower data with GPS, Wi-Fi networks, and other information culled from photos, videos, and other sources: ‘That lets Android pinpoint users to a single building, rather than a city block.’” “The information was used to manage Google’s ‘push’ notifications and messages sent to users on their Android phones, **enabling the company to track ‘whether an individual with an Android phone or**

⁹⁵ Ibid., pg. 98.

⁹⁶ Ibid., pg. 117.

⁹⁷ Ibid., pp. 242-243.

⁹⁸ Ibid., pp. 243-244.

running Google apps has set foot in a specific store, and use that to target the advertising a user subsequently sees.”⁹⁹

Professor Zuboff also discusses that Google’s Location History system is a product of the corporation’s global mapping operations. Though it has been active for over a decade (prior to 2019), it was first revealed to the public in 2015 as “Your Timeline” – a feature that allows you to “visualize your real-world routines.” Google said that “Your Timeline” is private and visible only to you and that you control the locations you keep, but they use your location data to target ads.¹⁰⁰

Professor Zuboff also discussed third-party products, providing the example of the French non-profit Exodus Privacy, which along with the Yale Privacy Lab identified 44 trackers in more than 300 apps for Google’s Android platform, some of which are also produced for Apple systems.¹⁰¹ “Even the most innocent-seeming applications such as weather, flashlights, ride sharing, and dating apps are ‘infested’ with dozens of tracking programs that rely on increasingly bizarre, aggressive, and illegible tactics to collect massive amounts of behavioral surplus ultimately directed at ad targeting...for example...users installing ‘Bottin Gourmand,’ a guide to restaurants and hotels in France, would thus have their physical location tracked via retail outlet speakers as they move around Paris...**the research findings indicate that the always-on tracking is impervious to the Android ‘permissions system,’ despite its promise of user control.**¹⁰²

Professor Zuboff discusses that The Register, a UK tech news website, revealed in 2016 that the Google Play store (pre-installed in Android phones) continuously checked a user’s

⁹⁹ Ibid.

¹⁰⁰ Ibid.

¹⁰¹ Ibid., pg. 137.

¹⁰² Ibid.

location, sending that information to the user’s third-party apps as well as to Google’s own servers.¹⁰³ A security researcher was shocked¹⁰⁴ when his phone prompted him to download the McDonald’s app the minute he entered the restaurant, and he later discovered that Google Play had monitored his location thousands of times.¹⁰⁵

Professor Zuboff also discusses Google Street View. Google’s “privacy counsel” announced the launch of this new service in 2007, writing in a blog post that “people don’t have the same expectation of privacy [in public spaces] as they do in their homes.”¹⁰⁶ In 2010, the German Federal Commission for Data Protection found that Google’s Street View cars were secretly collecting personal data from private Wi-Fi networks as they roamed. Google conceded it was collecting “payload data,¹⁰⁷” which includes location data, names, telephone numbers, credit information, medical information, photos, and video files.¹⁰⁸ The German Commission concluded that such data packets could be combined to form a detailed profile of an individual, allowing them to be identified. The FCC also investigated, but Google said the decision to collect “payload data” was the decision of one employee (even though he was emailing superiors about it frequently). Google refused to provide documents to the FCC and ultimately defended themselves in the suit using a passage in a wiretap law.¹⁰⁹

Professor Zuboff also discussed Pokémon Go, which is a virtual reality game born out of Google Maps, launched in 2016. John Hanke, the same engineer Google blamed for Street View’s privacy abuses, was its chief engineer, working through Google subsidiary Niantic

¹⁰³ Ibid., pg. 154.

¹⁰⁴ <https://twitter.com/musalbas/status/775261347122671616>

¹⁰⁵

https://www.theregister.com/2016/09/12/turn_off_location_services_go_ahead_says_google_well_still_track_you/

¹⁰⁶ Zuboff, *supra* note at 13, pg. 141.

¹⁰⁷ <https://www.theguardian.com/technology/2012/apr/16/google-fined-fcc-street-view>

¹⁰⁸ Zuboff, *supra* note at 13, pp. 143-144.

¹⁰⁹ Ibid., pg. 146.

Labs.¹¹⁰ Niantic also produced a location-tracking bracelet for use in the game.¹¹¹ Once you download the app, it uses your GPS and smartphone camera to hunt virtual creatures called Pokémon. The game drove users through cities and towns – giving Google free, accurate map development as they moved.¹¹² Within a week of its release, the app was listed as the most downloaded and highest grossing, with more users than Twitter.¹¹³ *Buzzfeed* reporter Joseph Bernstein advised users to check how much data the app was collecting from their phones: “Like most apps that work with GPS in your smartphone, Pokémon Go can tell a lot of things about you based on your movement as you play. Pokémon Go’s incredibly granular, block-by-block map data, combined with its surging popularity, may soon make it one of, if not the most, detailed location-based social graphs ever compiled.”¹¹⁴

Professor Zuboff also discussed Google’s Ground Truth project. This was initiated in 2008, but only revealed after a 2012 FCC report.¹¹⁵ Ground Truth is a “deep map” that contains the detailed “logic of places” (i.e. every neighborhood/area imaginable). Getting the details right requires behavioral data from mobile devices.¹¹⁶ Google integrated its exclusive proprietary data from Street View to improve it. “Manik Gupta [a group product manager for Google Maps] acknowledges that location signals could also be a good source of other information, about turn restrictions, say, or one-way streets. But he declined to elaborate. ‘Google uses location in multiple ways, but there's nothing specific I can talk about beyond that,’ he said.”

¹¹⁰ *Ibid.*, pg. 150.

¹¹¹ *Ibid.*, pg. 311.

¹¹² *Ibid.*, pp. 311-313.

¹¹³ *Ibid.*, pg. 315.

¹¹⁴ *Ibid.*, pg. 317.

¹¹⁵ *In re Google Inc.*, File No. EB-10-IH-4055, April 13, 2012, Notice of Apparent Liability for Forfeiture, <https://s3.documentcloud.org/documents/351298/fcc-report-on-googles-street-view.pdf>.

¹¹⁶ Zuboff, *supra* note at 13, pg. 151.

Professor Zuboff also discussed Google’s vehicular monitoring.¹¹⁷ Google’s Chief Economist Hal Varian is quoted as saying, “Because transactions are now computer-mediated we can observe behavior that was previously unobservable and write contracts on it. This enables transactions that were simply not feasible before.” He then suggests “vehicular monitoring systems” will be a paradigm shift—companies can simply prevent a car from being started if monthly payments were not being made.¹¹⁸ Google already offers app developers a cloud-based “scalable geolocation telemetry system” using Google Maps that could help further similar monitoring systems.¹¹⁹

Professor Zuboff also discussed Sidewalk Labs. In 2015, Sidewalk Labs was first listed as a subsidiary of Google’s holding company, Alphabet. Its engineers installed several hundred free internet-enabled kiosks in New York City under the stated goal of combating “digital inequality.” Sidewalk’s CEO characterized the kiosks as “fountains of data” that will collect “other data, all of which can create very hyperlocal information about conditions in the city.”¹²⁰ Sidewalk Labs eventually developed Flow, a traffic management system that relies on Google Maps, Street View, and machine intelligence to capture and analyze data from drivers and public spaces. These analyses produce prediction products described as “inferences about where people are coming from or going,” which allows administrators to “run virtual experiments” that will improve traffic flow.”¹²¹ Sidewalk has expanded Flow to sixteen cities.¹²²

Professor Zuboff also discussed Google Advertising. She discusses that in Google’s early years, the data it collected from search queries was “haphazardly stored and operationally

¹¹⁷ Ibid., pg. 213.

¹¹⁸ Ibid.

¹¹⁹ Ibid., pg. 218.

¹²⁰ Ibid., pg. 228.

¹²¹ Ibid., pg. 229.

¹²² Ibid., pg. 231.

ignored.”¹²³ Amit Patel, a former Stanford graduate student interested in data mining, is credited with the groundbreaking insight into the value of Google’s data caches.¹²⁴ Zuboff says the discovery of this “behavioral surplus” produced a 3,590% increase in revenue in less than four years.¹²⁵ Soon after, behavioral data was put to work on the user’s behalf to improve search accuracy, speed, etc.—at this point Google’s AdWords team only had seven people.¹²⁶ She discusses that Google’s founders initially were wary of advertising on their platform: “we expected that advertising funded search engines will be inherently biased toward the advertisers and away from the needs of consumers...the issue of advertising causes enough mixed incentives that it is crucial to have a competitive search engine that is transparent and in the academic realm.”¹²⁷

Professor Zuboff discusses that this stance is the opposite of Google’s stance today; Google uses the exclusive behavioral data it receives from user searches to target advertising to those individuals.¹²⁸ Google maximizes its revenue by its ability to tell advertisers what the price per click will be, multiplied by the likelihood that someone will click on the ad (which Google figures out by analyzing user data).¹²⁹ Zuboff calls the multiplier “critical,” as Google has a near-monopoly on behavioral data and its future growth would depend on obtaining more of it.¹³⁰ Zuboff analyzed a patent application entitled “Generating User Information for Use in Targeted Advertising” and reports that Google began creating “user profile information” (UPI) data. UPI may be “provided by the user, provided by a third-party authorized to release user information,

¹²³ Ibid., pg. 67.

¹²⁴ Ibid.

¹²⁵ Ibid., pg. 87.

¹²⁶ Ibid., pg. 69.

¹²⁷ Ibid., pg. 71.

¹²⁸ Ibid., pg. 74-75.

¹²⁹ Ibid., pg. 77.

¹³⁰ Ibid.

and/or derived from user actions. Certain user information can be deduced or presumed using other user information of the same user and/or user information of other users.”¹³¹ At that time, scientists noted that users do not always voluntarily provide information due to privacy considerations; recognizing this as an issue with UPI.¹³² Professor Zuboff discusses that Google essentially passed along its data collection/advertising practices to Facebook when Sheryl Sandburg went to work for the company. Professor Zuboff discusses that in 2016 Google violated the pledge it gave to the FTC when it earlier allowed the company to acquire DoubleClick—saying in 2016 that a user’s DoubleClick browsing history “may be” combined with personally identifiable information from Gmail and other Google services.¹³³

Professor Zuboff also discusses other Alphabet/Google products. She discusses that Gmail was found to be scanning private correspondence upon its launch in 2004 to generate advertising.¹³⁴ She also discusses how Google chronicler Steven Levy noted that, “By serving ads related to content, Google seemed almost to be reveling in the fact that users’ privacy was at the mercy of the policies and trustworthiness of the company that owned the servers. And since those ads made profits, Google was making it clear that it would exploit the situation.” She also discusses that Alphabet’s home thermostat Nest was reportedly sharing sensitive personal information from one’s home to other devices, unnamed personnel, and third parties for analysis and advertising.¹³⁵ Finally she discusses that Google Now, the corporation’s first digital assistant

¹³¹ Ibid., pp. 77-79.

¹³² Ibid., pp. 79-80.

¹³³ Ibid., pg. 161.

¹³⁴ Ibid., pg. 47.

¹³⁵ Ibid., pg. 237.

was launched in 2015. It was initially a feature of Google search app for Android and iOS but has since become incorporated into the Google app and feed on smartphones.¹³⁶

E. 2019 New York Times Location Data Study

In 2019, an investigative team from *The New York Times* obtained a dataset of location data for 12 million Americans containing over 50 billion location ‘pings.’ Each ping, representing a moment in time when a smartphone’s location was recorded, contained precise location coordinates associated with a specific smartphone.¹³⁷ The data was provided anonymously by an employee at a location data company and covered several major U.S. cities for several months from 2016 to 2017. According to the reporters, “[i]n the cities that the data file covers, it tracks people from nearly every neighborhood and block, whether they live in mobile homes in Alexandria, Va., or luxury towers in Manhattan.”

While this data was “anonymized” in the sense that it was not directly linked to individuals by name, address, or even phone number, individuals could be tracked in the dataset through other static identifiers such as their phone’s device IDs.¹³⁸ And because precise geolocation coordinates allow anyone to create a map of an individual’s movements, it is possible to isolate an individual device ID from a location dataset and map its specific movements over time. Since most of us have typical, routine travel patterns each day, reverse-identifying individuals through their location data isn’t unusually difficult.

That is precisely the challenge that the *Times* investigatory team took upon themselves. This dataset did not contain the fuller set of data that companies, including Google, often have on

¹³⁶ <https://www.extremetech.com/mobile/252721-google-announced-redesigned-feed-replacement-google-now>

¹³⁷ Stuart Thompson and Charlie Warzel. “The Privacy Project: Twelve Million Phones, One Dataset, Zero Privacy.” *The New York Times*. December 19, 2019. Available at: <https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html>

¹³⁸ Device IDs are a unique ID assigned to each phone, similar to a serial number.

individual consumers that essentially saves them the challenge of having to reverse-identify individuals through their location data; many of these companies either already know exactly to whom the data belongs, or are able to gather enough additional data to infer that knowledge.¹³⁹ The *Times* team instead zeroed in on individual phones in different areas, including high-security areas in Washington D.C. such as the White House and the Pentagon.¹⁴⁰ In the course of their reporting, the team uniquely identified dozens of individuals, who they contacted to share their findings. The reporters conducted a deep dive into the California city of Pasadena, where they identified and interviewed several residents, including a Los Angeles County Sheriff’s deputy, a high school principal (who was shown how the students in his own school were traceable), and a scientist at NASA’s Jet Propulsion Lab. The team identified the individuals through their location patterns, contacted them, and then met them in-person to show them maps of their aggregated data and ask questions about the experience. Most, understandably, were disturbed and upset. Repeatedly, the question of consent arose: no one recalled ever providing consent to that level of ongoing, detailed tracking of their personal lives.

I find this project reliable in its discussion of the level of location detail that is collected by platforms and advertisers and as a study of how location data can be used to track individuals. It also demonstrates that the anonymity we enjoy by assuming we are an unknowable single point in a very large database is anonymity by *obscurity*, not true anonymity.¹⁴¹ This is not the first study to demonstrate that it is possible to identify individuals from data that appears to be

¹³⁹ Jon Keegan and Alfred Ng. “There’s a Multibillion-Dollar Market for Your Phone’s Location Data.” *The Markup*, Sept. 30, 2021. <https://themarkup.org/privacy/2021/09/30/theres-a-multibillion-dollar-market-for-your-phones-location-data>.

¹⁴⁰ Stuart Thompson and Charlie Warzel. “The Privacy Project: How To Track President Trump.” *The New York Times*. Dec. 20, 2019. Available at: <https://www.nytimes.com/interactive/2019/12/20/opinion/location-data-national-security.html>

¹⁴¹ Hartzog, Woodrow, and Frederic Stutzman. “The Case for Online Obscurity.” *California Law Review*, vol. 101, no. 1, California Law Review, Inc., 2013, pp. 1–49, <http://www.jstor.org/stable/23409387>.

anonymized.¹⁴² With location data, we have an illusion of anonymity as long as no one is looking. But this is only an illusion. Location data allows companies like Google to know exactly who we are and where we go. They use this data to target ads, fine-tune search results, and make inferences about us that are neither fully transparent nor directly connected to a one-time exchange of location data for information, such as driving directions. This data is also of enormous interest to law enforcement, and questions about precise location tracking by the police have even reached the Supreme Court.¹⁴³ Many other commercial actors are eager to access location data. Insurance companies want to know where you drive or travel; debt collectors have purchased mobile location data from cell phone providers in order to locate debtors; all manner of companies want to serve you location-based ads.¹⁴⁴

VI. HARMS FROM LOCATION DATA TRACKING

Google’s systematic collection, storage, and processing of consumers’ personal location harms consumers in ways that they cannot reasonably avoid. Some of the harms are possible with the collection of geolocation in general. But these harms are particularly salient here, given the conduct of Google as alleged here by the State.

¹⁴² See generally: A. Narayanan and V. Shmatikov, “Robust de-anonymization of large sparse datasets,” in 29th IEEE Symposium on Security and Privacy, 2008, pp. 111–125; Michael Barbaro and Tom Zeller, Jr. “A Face Is Exposed for AOL Searcher No. 4417749.” *The New York Times*, Aug. 10, 2006.

<https://www.nytimes.com/2006/08/10/learning/featuredarticle/20060810thursday.html>; Paul Ohm. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review*, Vol. 57, p. 1701, 2010.

¹⁴³ *Carpenter v. United States*, 138 S. Ct. 2206 (2018). I am aware that the Arizona Supreme Court in a case called *State v. Mixton*, 478 P.3d 1227 (Ariz. 2021) concluded that the Arizona constitution did not create an exception to the “third-party” doctrine for IP addresses, and distinguished IP addresses from location tracking, as was the issue in *Carpenter*.

¹⁴⁴ Keegan and Ng, *supra* note 139.

A. Data Collection Implicates Privacy Concerns

The collection of data about us, including location data, by companies, the government, and even other individuals raises questions about our *privacy*. Privacy can be a complex topic, but when we are talking about data privacy, it is most commonly thought of as Professor Alan Westin described it: *having control over the information others know about you*. Some people think it’s specifically about having or keeping secrets, which is why they will declare: “I have nothing to hide, so I don’t need privacy.” But privacy isn’t only about hiding secrets, illegal activities, unpopular opinions, or lifestyle choices that others might not approve of. It is about having the *autonomy*—the freedom—to make choices about your own life, and having others respect those choices. It is about you, as an individual, having the freedom to decide what you want others to know about you, and what you wish to share with them. It is also about you having the ultimate choice over what parts of your life you feel are fair and appropriate to share with companies for commercial decisions.

Privacy harms can often be challenging to recognize because, unlike a direct physical or financial injury, they can be indirect, aggregate, or occurring over time rather than at a single instance. According to law professors Danielle Citron and Daniel Solove, two highly respected experts on privacy, “[f]or many privacy harms, the injury may appear small when viewed in isolation, such as the inconvenience of receiving an unwanted email or advertisement or the failure to honor people’s expectations that their data will not be shared with third parties. But when done by hundreds or thousands of companies, the harm adds up.”¹⁴⁵ In this case, Citron and Solove’s logic also applies “when done hundreds of thousands of times” by the same company (in Google’s case, perhaps billions of times).

¹⁴⁵ Danielle Keats Citron and Daniel Solove, *Privacy Harms*, 102 B.U. L. Rev. 793 (2022).

Citron and Solove identify seven groups of individual privacy harm: physical, economic, reputational, psychological, discriminatory, relational, and to individual autonomy. The harms posed by the long-term collection and aggregation of location data are primarily autonomy-based, discriminatory, and economic in nature, though depending on how location data is used or disclosed it could cause physical, relational, and reputational harms as well. A key argument the authors make is that even though many of the harms individuals experience from the misuse of data are intangible and the downstream effects are difficult to track, this doesn't lessen the experience of harm. My own qualitative research talking with individuals supports this perspective; while in some cases one can draw a direct line from a data disclosure to an experience of harm, in many instances it is subsequent experiences that stem from a disclosure that contribute to an experience of harm.¹⁴⁶

An example of aggregated, downstream effects from data collection is the creation of *information asymmetries* between individuals and the companies that collect their data. An information asymmetry is the state where one party has access to far more information about the other than vice versa. This imbalance in a commercial context means that companies can use this information to influence your choices and decision-making not only by serving you precisely targeted ads based on things you've done or places you've been, but also by making predictions about you, sometimes even about things you are barely aware of yourself, or intimate things you've not shared with anyone. Always-on, systemic surveillance of our lives upends our autonomy and it creates a situation of unfairness through information asymmetry.

Pregnancy is a common life event where information asymmetry occurs. Because a woman's pregnancy necessitates both lifestyle changes and the need for new products and services (e.g., maternity clothing, baby gear), marketers have a keen interest in influencing those

¹⁴⁶ King, *supra* notes 14 and 58.

new and developing choices. Pregnancy also produces changes in people’s daily routines that correlate not only with the stage of a mother’s pregnancy, but also with socioeconomic factors such as education and income.¹⁴⁷ These distinctive characteristics of pregnancy have allowed marketers to identify and target women giving birth, even as these women never disclosed their pregnancies. In 2012, the reporter Charles Duhigg documented how the national retailer Target had developed a way to predict that customers were pregnant at a very early stage based on changes in their purchasing patterns.¹⁴⁸ Any customer who shopped regularly at Target was assigned a Guest ID, under which Target amassed information about “which part of town you live in, how long it takes you to drive to the store,” and a host of other demographic information that Target declined to disclose in full.¹⁴⁹ The retailer then used this data to build a prediction algorithm¹⁵⁰ and send advertising mailers to households with babies on the way, featuring pregnancy and baby products. Famously, after a teenaged girl received one of these customized mailers at home, her father complained to the company, only to find out after the fact that his daughter was, in fact, pregnant.¹⁵¹ Other women have complained about the ways in which online companies discover they are pregnant, many times before they are ready to even tell anyone else, and then shower them with ads, sometimes revealing their pregnancies to others

¹⁴⁷ <https://ehjournal.biomedcentral.com/articles/10.1186/1476-069X-12-86>

¹⁴⁸ Charles Duhigg. “How Companies Learn Your Secrets.” *The New York Times Magazine*, Feb. 16, 2012. <https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html>

¹⁴⁹ https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=1&hp; see also <https://techland.time.com/2012/02/17/how-target-knew-a-high-school-girl-was-pregnant-before-her-parents/>

¹⁵⁰ An algorithm is a step-by-step computational process for achieving a certain task or solving a certain problem. A prediction algorithm takes in data and, based on that data, outputs a projected result.

¹⁵¹ See *supra* note 149.

before they are ready, to the point where some have tried to keep their pregnancies a secret from online marketers.¹⁵²

Others also think about the privacy of personal information in terms of its appropriate use. After all, we are often okay with sharing the same data about ourselves in one situation, but not another. For example, a woman who is newly pregnant might be fine sharing this information with a doctor and a family member, but not with others, such as co-workers. This concept is called *contextual integrity*,¹⁵³ and it captures the idea that many of us, for example, are okay with sharing our location data at a single point in time in order to receive useful information. However, the collection of our location data outside these contexts can violate contextual integrity. For example, the developer of a flashlight app was fined by the Federal Trade Commission because it used its “free” app (i.e. one that did not charge money to download or use) as a pretext for collecting as much data as possible about its users, none of which was needed in order for the app to work as a flashlight.¹⁵⁴ Of course, this app is not really “free”—the user pays for the app through all of the personal data they turn over to the company.

Context is important. When you make a request for information that either necessitates or is improved by access to your real-time location (e.g., “where is the nearest bus stop?”), that may be considered a *contextually appropriate* request, meaning that the request for location by the app is appropriate for the context in which you are providing it. These contextual, real-time exchanges of location data for information constitute the experience that many of us have with

¹⁵² Janet Vertesi. “My Experiment Opting Out of Big Data Made Me Look Like a Criminal.” *Time*, May 1, 2014. <https://time.com/83200/privacy-internet-big-data-opt-out/>

¹⁵³ Helen Nissenbaum. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford: Stanford University Press, 2009.

¹⁵⁴ <https://www.ftc.gov/news-events/news/press-releases/2014/04/ftc-approves-final-order-settling-charges-against-flashlight-app-creator>; *In re Goldenshores Techs., LLC*, No. 132-3087, 2014 WL 1493611 (Fed. Trade Comm’n Mar. 31, 2014) (alleging failure to disclose the collection of geolocation information to be an unfair and deceptive trade practice).

mobile apps, and it is one that most find appropriate. If a mapping app doesn't know where I am at right now, how can it provide me directions to the nearest park? In order to receive those directions, providing immediate access to one's general or specific geolocation to a mobile app allows one to receive as accurate directions as possible. At the same time, the State makes claims here that Google collects stores and uses location data in a way that is not *contextually* appropriate. When a user has paused (or never enabled) a setting called "Location History," the consumer would not expect Google to collect location history through some other setting called "Web & App Activity." This is demonstrated by the Associated Press Article and the reaction that followed. Along the same lines, even if user expects Google to use a query to return a location-relevant response, that does not mean a user expects Google to *store* that location information. As yet another example, if a user provides Google with their own location, that does not necessarily mean that the user has agreed to allow Google to use that information for tracking others.

B. The Paradigm Shift Towards Always-On Location Collection Implicates Privacy Concerns Specifically

It did not take long after the introduction of smartphones for questions to arise over the potential sensitivity and privacy implications of mobile location data: who had access to it, what it was being used for, and how long it was being kept. Prior to their introduction, digital companies at best may have had a general idea of where you might be located based on the internet protocol (IP) address you used to access the internet. Even using early versions of mobile web browsing at best provided a very general idea (often incorrect) of where an individual was located in real time. A company such as Google might be able to generalize one's location history based on collecting the various IP addresses one used when accessing their

services, but was limited to your desktop and laptop computer use, as well as whether you signed into their services, or used the same browser repeatedly. In contrast, smartphone users with location services enabled became individually, uniquely knowable, not only in terms of what they searched for and what apps they used, but also where they did these things: at home, work or school, and everywhere else they traveled.

This level of location-based knowledge raised alarm bells for privacy and civil liberties advocates as it became clear that the level of actual, real-time knowledge of where individuals traveled throughout their days allowed for an unprecedented level of individual surveillance. In comparison, if law enforcement wanted to track an individual that closely, they would need to appear before a judge to request a warrant for permission. Smartphones facilitated intimate surveillance by private actors, and it was not clear whether the public broadly understood that this was happening, as well as what happened to that data after it was collected.

A number of public scandals around location collection began to make these concerns material. In 2010, Google was found to be engaged in mapping Wi-Fi networks via the cars they deployed to drive around neighborhoods capturing the image data the company used to create Google StreetView.¹⁵⁵ The cars scanned for the networks as they took photos, which allowed them to create maps of Wi-Fi networks to aid in creating precise location maps in the event that a smartphone had GPS disabled, or GPS signals were poor.¹⁵⁶ The following year, 2011, Google settled with the Federal Trade Commission over privacy concerns with their short-lived social networking service, Google Buzz, which created public-facing contact lists based on a user's

¹⁵⁵ <https://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html>

¹⁵⁶ <https://support.google.com/maps/answer/1725632?hl=en>

most frequently used Gmail contact without their consent.¹⁵⁷ As part of that settlement, Google agreed to a consent decree that ordered the company not to “misrepresent in any manner, expressly or by implication...the extent to which respondent maintains and protects the privacy and confidentiality of any covered information, including, but not limited to, misrepresentations related to: (1) the purposes for which it collects and uses covered information, and (2) the extent to which consumers may exercise control over the collection, use, or disclosure of covered information.”¹⁵⁸ The consent decree defines “covered information” as “information respondent collects from or about an individual, including, but not limited to, an individual’s: (a) first and last name; (b) home or other physical address, including street name and city or town; (c) email address or other online contact information, such as a user identifier or screen name; (d) persistent identifier, such as IP address; (e) telephone number, including home telephone number and mobile telephone number; (f) list of contacts; (g) physical location; or any other information from or about an individual consumer that is combined with (a) through (g) above.”¹⁵⁹

Similarly, in April 2011 researchers Alasdair Allan and Pete Warden discovered an unencrypted cache of location data stored on iPhones that revealed the geolocation information of hundreds of Wi-Fi hotspots and cell towers that the phones contacted during their use.¹⁶⁰ Some of this data was stored for up to a year, and in some instances it was even collected against users' affirmative decision to disable location services. Notably, the collection was an "open

¹⁵⁷ Nicholas Carlson. “WARNING: Google Buzz Has A Huge Privacy Flaw.” *Business Insider*, Feb. 10, 2010. <https://www.businessinsider.com/warning-google-buzz-has-a-huge-privacy-flaw-2010-2>

¹⁵⁸ *In the Matter of Google Inc.*, Consent Decree, Federal Trade Commission, 2011.

¹⁵⁹ *Ibid.*

¹⁶⁰ See: Jennifer Valentino-DeVries. “What Your Phone Knows About You.” *The Wall Street Journal*, April 20, 2011. <https://www.wsj.com/articles/BL-DGB-22372>; Alasdair Allen and Pete Warden. “Got an iPhone or 3G iPad? Apple is recording your moves.” *O’Reilly Radar*, April 20, 2011. <http://radar.oreilly.com/2011/04/apple-location-tracking.html>.

secret" in the security community at the time of its public disclosure.¹⁶¹ Apple claimed the data was anonymous and encrypted, so that Apple could not identify a user from the geolocation information being sent back to the company. But as discussed earlier in this report, because location data can identify where we live and work, it is questionable whether collections of data from a single phone over time can be truly anonymized.

Apple claimed the collection of this data was unintentional, and fixed the issue in iOS 4.3.3. However, the verification that mobile platform providers were collecting and storing location data prompted the U.S. Senate Judiciary Subcommittee on Subcommittee on Privacy, Technology and the Law to hold a hearing in May 2011 entitled "Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy."¹⁶² Both Google¹⁶³ and Apple¹⁶⁴ executives testified at this hearing, with Alan Davidson (Google's Director of Public Policy at the time) stating that "we don't collect any location information — any at all — through our location services on Android devices unless the user specifically chooses to share this information with Google . . . [a]nd even after opting in, we give users a way to easily turn off location sharing with Google at any time they wish."

Despite Mr. Davidson's testimony, the facts here present a different picture. For example, Dr. Nielson's Declaration, as well as the other evidence discussed above, indicate that Google has long collected location information even when consumers disable the relevant settings. There is no "opt out" particularly for IPGeo and [REDACTED] The Complaint (at paragraph 89) quotes testimony from three Google witnesses (Rothfuss, Berlin and Hennessy) who confirm that

¹⁶¹ Alasdair Allen and Pete Warden. "iPhone Tracking: The Day After." O'Reilly Radar, April 21, 2011, <http://radar.oreilly.com/2011/04/iphone-tracking-followup.html>.

¹⁶² <https://www.judiciary.senate.gov/meetings/protecting-mobile-privacy-your-smartphones-tablets-cell-phones-and-your-privacy>

¹⁶³ <https://www.judiciary.senate.gov/imo/media/doc/11-5-10%20Davidson%20Testimony.pdf>

¹⁶⁴ <https://www.judiciary.senate.gov/imo/media/doc/11-5-10%20Tribble%20Testimony.pdf>

a user cannot prevent Google from using an IP address as an input, which (according to Dr. Nielson) is then ingested by Google IPGeo and [REDACTED] services. In this context, it is also important to call out the explanation of Google engineer Blake Lemoine (quoted in paragraph 117 of the Nielson Declaration), who explains that Google built a [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Mr. Davidson’s suggestion that Google gives “users a way to easily turn off location sharing with Google at any time they wish” is also inconsistent with the State’s allegations I describe above and my own experience. As noted above, the AP Article explains how people believed their location was not being tracked since something called “Location History” was disabled and, yet, Google continued to track their location through WAA. Google’s internal documents suggest Google has long known that its location sharing settings are not so “easily turned off.” Even today, Google does not take “no” for answer and, instead, applies “off means course” when users disable their device location.

Google’s conduct here is harming both the users’ privacy and autonomy. Google has completed the shift to “Always-On Location Collection.” But Google also creates a web of settings that suggest to users that they have a choice to disable location tracking when ultimately there was no “opt-out.”

C. How Google’s Location Data Collection Harms Privacy

There are several reasons why Google’s systematic collection of one’s location data causes concerns and harms both individuals and society at large.

Location Data Reveals Sensitive Locations and Activities: Many of us forget that while we may have fairly routine travels from day to day, we do visit places that can cause concern if known to others or viewed out of context. This can include: health professionals (doctors, clinics, mental health practitioners), lawyer’s offices, places of worship, political gatherings, or even personal relationships that you want to keep private or avoid the appearance of impropriety. If our phones are tracking our location when we visit these places, then someone has a record of it. If our location data is kept indefinitely, then it can be easy to forget that our phones have kept a record of these travels. To put a finer point on it, location tracking can disclose sensitive work matters, including meeting with key customers and potential customers (which could disclose their identity). It could also disclose job interviews with prospective employers, which employees may want to keep confidential. There are also some people who have sensitive jobs for the government as illustrated by the *New York Times* investigation.

Location data can also disclose sensitive personal activity about a person and their family (e.g., medical visits, visiting political gatherings, visiting a lawyer’s office, religious gatherings). One example could be visiting a child psychologist. Many parents may not want that fact stored by a company indefinitely simply because they traveled to that location. The same is true for a person’s own medical visits, such as visiting a marital therapist or fertility clinic, for example. Also, people with non-obvious medical conditions may not want to share that simply by having which particular doctor’s offices they visit be tracked, or even how often they visit any type of medical office for fear that they could be inferred as not healthy.

Other examples of sensitive data are when the data collection reveals where someone is spending most of their time. People who are going through a non-public separation with their spouse or significant other and not staying at their normal residence or visiting a divorce attorney may not want that tracked and stored. Another example is people who attend a political gathering, meeting, or protest, may not want that attendance to be stored forever by a company for fear of adverse effects on employment, promotion, or even being “cancelled” (i.e., publicly shamed). There are also unknown or unquantifiable harms, such as what things could be inferred from systematic, location monitoring (either by itself or in conjunction with other data), such as spending habits that consumers may want to not have tracked and stored.

To be sure, some consumers may not mind this information being tracked—at least sometime and in the appropriate context. But there is a fundamental difference between consenting to tracking (especially at a specific time or for a specific purpose) versus having it happen systematically, including in the background, without consumer consent.

As discussed above, Google infers sensitive location information about users—including their home and work location—even when a user turns off all device-location settings. According to the deposition testimony of Jack Menzel cited in paragraph 93 of the Complaint, the only way for Google *not* to infer a user’s home and work is for that user to set “home and work to arbitrary locations.”

Location Data Poses Harm To Vulnerable Populations: Even if you are not personally concerned about the collection and use of your location data, there are people for whom their tracked location makes them vulnerable: undocumented people, people in abusive relationships, people protesting the government, to name a few. There are cases where the U.S. government and law enforcement agencies have purchased location data from commercial providers in order

to track both individuals and specific groups.¹⁶⁵ The widespread, unconstrained collection of location data can put many people at risk who might otherwise not assume they are vulnerable.

Moreover, through IPGeo and [REDACTED] (as discussed above), not only does Google collect this location information, but Google also coopts other witting users to help report the location of their relatives, friends, neighbors or other people who happen to be nearby.

Location Data is Collected and Used With A Lack of Transparency: A tremendous challenge with location tracking is the lack of transparency for smartphone users that it is even happening, as well as who is doing it, and how long location data is being kept. Most of us would agree that we didn't consent to being systematically tracked, and such data being stored, simply because we wanted to obtain directions or look up the nearest grocery store. However, smartphone app permissions as well as our phone's mobile operating system location settings can enable exactly that kind of tracking even when we only intended for the use of our location for a specific context and for a specific moment in time. It is through that systematic collection that companies are able to create detailed dossiers about who we are, where we go, and what they think our preferences are.

Furthermore, this data can then be used to develop extensive profiles and inferences about individuals far outside the original context of collection, exacerbating concerns about privacy, autonomy and unfairness. This lack of transparency can be a source of anxiety for those who are aware that tracking occurs but who don't understand how to curtail or minimize it. For those who do attempt to minimize tracking through location settings or privacy settings, those tools can provide a false sense of security when they do not perform as promised. It is precisely

¹⁶⁵ Laura Hecht-Felella. "Federal Agencies Are Secretly Buying Consumer Data." The Brennan Center, April 16, 2021. <https://www.brennancenter.org/our-work/analysis-opinion/federal-agencies-are-secretly-buying-consumer-data>.

this lack of transparency that led to consumer concerns in recent years about whether large platforms like Google are actively listening to them through their phones and secretly recording their conversations.¹⁶⁶ The combination of collecting one’s geolocation in real time, combined with additional forms of data such as search terms, has created a data ecosystem where it can sometimes seem as if you have just thought about something, or discussed something with a friend or relative, and your smartphone or browser responds with an ad targeted to you on precisely that topic, sometimes within minutes.

The anxiety around Google’s lack of transparency was apparent from the blog post that led to the Associated Press Article, as well as in the press that came after. In her May 2018 and June 2018 blog posts, Dr. Shankari described her unease when she realized Google was still tracking her location. In the May 2018 post, she explained that the manner in which she was being tracked is “creepy and wrong.” In the June 2018 post, she described similar sentiments: “I had already turned off all of its permissions, directly from the app settings...this seems unambiguously wrong.” She proceeded to “review the facts,” noting that (i): “The Google app cannot be uninstalled or disabled;” (ii): “The Google app does not have a built-in control for location tracking but says that location data collection should be modified in the app settings;” (iii): “I have explicitly stated, through app settings, that I don’t want the Google app to have access to my location;” (iv): “The Google app has access to my location, as shown by the prompts it generates which include my location.”

¹⁶⁶ Coco Khan. “Is My Phone Listening To Me? We ask the expert.” *The Guardian*, Oct. 29, 2021. <https://www.theguardian.com/lifeandstyle/2021/oct/29/is-my-phone-listening-to-me-we-ask-the-expert>; Tatum Hunter. “Ask Help Desk: No, your phone isn’t listening to your conversations. Seriously.” *The Washington Post*, November 12, 2021. <http://washingtonpost.com/technology/2021/11/12/phone-audio-targeting-privacy/>.

As of Day 4 after the Associated Press Article, Google documents show that it was re-tweeted about thousands of times and was picked up by more than 60 new outlets.¹⁶⁷ Google also tracked 187,007 “Social Shares,” including Facebook, and tracked the “sentiment,”¹⁶⁸ or qualitative reactions, to the post. Google shows that “69% of the coverage mentioned *the lack of user consent / creepy factor*,” whereas “33% of coverage mentioned *“misleading controls.”*”¹⁶⁹ Google’s internal documents highlight a comment from the Director of Cybersecurity for the Electronic Frontier Foundation: “When you tell Google to stop tracking your location, it should stop tracking your location. Period.”¹⁷⁰ It also highlighted tweets from across the political spectrum, including from “conservative”: “This is literally fraud, it’s time for massive class action lawsuits against Google,”¹⁷¹ and from (Democratic) Senator Richard Blumenthal: “It should be simple—‘off’ means ‘off.’ Google’s relentless obsession with following our every movement is encroaching & creepy. I’ve called for an FTC investigation into its persistent privacy invasions.”¹⁷²

This is particularly relevant to Google. Documents obtained by the State in this case show that Google has a goal of gaining “perfect” (i.e., complete) knowledge about its users. Google described its location platform as being complete when its knowledge of its users’ whereabouts is perfected: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

¹⁶⁷ GOOG-GLAZ-00001422.


¹⁶⁸ GOOG-GLAZ-00001422.

¹⁶⁹ GOOG-GLAZ-00001422.

¹⁷⁰ GOOG-GLAZ-00001422 at 1424.

¹⁷¹ GOOG-GLAZ-00001422 at 1424.

¹⁷² GOOG-GLAZ-00001422 at 1428.

¹⁷³ Google also logged tweets from key business leaders, journalists, celebrities, and current and former government officials, including a tweet from the former FTC CTO.¹⁷⁴

D. Location Data Collection Can Also Cause Financial Injuries to Consumers

Threats to autonomy and discrimination are not the only harms implicated by continuous location tracking. There are also financial harms to consumers, though again the harms may not be immediate or direct.

Smartphone Tracking Requires Data Resources: Not all consumers over the past decade or longer have had unlimited data plans for their smartphones. Instead, they pay to use data or they pay for a certain amount of data per month. The transmission of location data may impact consumers' mobile data plans. Although the amount may vary, and be relatively small for each consumer, this is still a distinct harm that impacts broad swaths of smartphone consumers.¹⁷⁵

Ad Targeting—The Visible and The Invisible: Like the pregnancy example discussed above, some are concerned about being targeted for ads based on their location data, in terms of the places they visit but also what location allows Google to infer about them. This includes children, who can be more susceptible to marketing messages than adults. But an important aspect to understand about ad targeting is that it is not only about seeing ads, it is also about what you don't see. There are concerns about potential discrimination regarding the types of information that you aren't shown based on your demographics and where you live. For example, you may be charged more for a product based on where marketers think you live, or

¹⁷³ GOOG-GLAZ-00283334.

¹⁷⁴ GOOG-GLAZ-00001422 at 1429.

¹⁷⁵ See, e.g., Oracle White Paper, at p. 55; AZAGKoernerPRR000111.

not shown particular job ads you might have actually wanted to see based on factors such as your age, location, gender, race, or ethnicity.¹⁷⁶ Many people can identify when an ad feels creepy because it is very precise, sometimes about a topic that you might have just been discussing or thinking about, as the phone listening example mentioned above demonstrates. What can be harder is to understand when you are excluded based on these factors because the exclusion can be invisible to you. Google has internal documents [REDACTED]

[REDACTED] .¹⁷⁷

Consumers Are Unable to Financially Benefit From the Use of Their Location Data:

The trade-off of access to free services in exchange for the use of one’s personal data has been the primary business model of the internet for two decades. However, as large platforms, particularly Google, have gained immense fortunes based on their users’ data, this business model has received increased scrutiny.¹⁷⁸ Governor Gavin Newsom of California raised the issue in 2019 of whether consumers should receive data dividends directly in some form from the companies that collect and monetize their data.¹⁷⁹ Other actors have suggested that individuals should be able to receive direct financial benefit from the use of their data by licensing it or even selling it to companies.¹⁸⁰ However, the domination of data markets by large platforms such as Google makes it nearly impossible for these competing concepts to gain traction. Thus, even if

¹⁷⁶ Amit Datta, Michael Carl Tschantz, and Anupam Datta. “Automated Experiments on Ad Privacy Settings: A Tale of Opacity, Choice, and Discrimination.” Privacy Enhancing Technologies Symposium (PETS), 2015.

¹⁷⁷ GOOG-GLAZ-00312666, at 667 [REDACTED]

[REDACTED]; GOOG-GLAZ-00224887, at 891 (resume of Google Software Engineer, which states HHI targeting “uses precise location (GPS and real time IPGeo) as input and maps the location to household income.”); GOOG-GLAZ-00274982: [REDACTED].

¹⁷⁸ Chris Hoofnagle and Jan Whittington. Free: Accounting for the Costs of the Internet’s Most Popular Price. 61 UCLA L. Rev. 606 (2014).

¹⁷⁹ See generally: <https://www.datadividends.org/>

¹⁸⁰ See generally: <https://www.datadividendproject.com/>

consumers were willing to pay for access to services, or were open to licensing or selling their data in exchange for services, absent government intervention it is unlikely consumers at scale will be able to benefit from these proposals.

As noted above, after Google aggregates the location signals, the internal [REDACTED] service then “markets” the location information to other internal Google clients. Google says it does not “sell” location information, but one internal client “markets” the location information other internal clients. This shows that the location data is valuable and marketable.

E. Other Factors Affecting Harm

There are other factors that, when violated, also aggravate harm to consumers. The first is data minimization, which is a long-standing principle of privacy protection.¹⁸¹ Similarly, the International Association of Privacy Professionals describes the collection-limitation principle clearly: “The Collection Limitation Principle: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.”¹⁸² Systematic collection of location information, where far more information than is needed to provide the service occurs, is contrary to the principle of data minimization.

Second, storage of user location data increases the harms identified above from collection. I understand Google not only collects but stores user location data. For some of the settings, I understand Google offers users the ability to go into their Google Account and delete past location data collected by Location History and Web & App Activity, as well as pause the

¹⁸¹ See FTC Staff Report, *Internet of Things: Privacy and Security in a Connected World*, 34, 36 (Jan. 2015), <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>

¹⁸² <https://iapp.org/resources/article/fair-information-practices/>

ongoing collection of location data by those products/settings. Additionally, in 2020 Google introduced a feature that defaults new accounts to auto-delete Location History and Web & App Activity data after eighteen months. However, these options do not cure the past harms from location tracking. Further, as discussed more below, default settings are very powerful because consumers rarely modify them. Because certain location data collection is on by default (e.g., via Web & App Activity), consumers are often unaware that this location collection is taking place unless proactively prompted to review it. Even an eighteen-month window of auto-deletion still means continuous location tracking; it just means that the aggregated history now no longer remains stored forever.

Further, even if a consumer goes in after the fact and deletes location data, that does not necessarily eliminate the processing, profiling, and inference generation about the consumer that has already occurred; it simply prevents such activities from being updated with new data in the future. Allowing the consumer to go in after the fact and delete data that has already been processed to build an advertising profile does not cure the harm, nor may it absolutely prevent similar forms of processing, profiling, and inference generation in the future unless the profiles and inferences themselves are also deleted. While Google has recently introduced features such as the privacy check-up, these features do not explain to consumers the risks and harms they may experience if they do not engage these features. Nor do they provide consumers with a clear method for “cleaning the slate” by eliminating all processed data from their accounts. Also, it is my understanding that these deletion options do not apply to all settings, such as IPGeo and

██████████.

F. Tracking Harms Are Not Reasonably Avoidable By Consumers

I also conclude that these harms are not something that consumers can reasonably avoid. I understand that that injury to consumers is considered reasonably avoidable if consumers have a reason to anticipate the impending harm and the means to avoid it, or if consumers are aware of, and are reasonably capable of, pursuing potential avenues toward mitigating the injury after the fact. That is not the case here.

Looking back over the progression of smartphones, the year 2011 marked a turning point in discussions about the privacy implications of mobile location data. Advocates and policymakers were raising concerns whether smartphone users had a good understanding of what data was being collected about them (including location data), whether companies had clearly obtained consent for the collection of this data, and whether they communicated their uses of this data to the public. There are three specific areas where these concerns were raised: APIs that helped developers leverage an individual's location data, the notice and consent process for collecting location data, and the inertia of defaults that enabled greater data collection. All told, these different parts of these systems worked together to intentionally collect location information by design.

1. Smartphone APIs: How All-or-Nothing APIs Enabled Widespread Location Collection

From the start, smartphones were designed to enable widespread data tracking. A crucial contributor to this design were the mobile APIs that granted third party app developers access to an individual's location data. Both Android and iOS launched with the competitive goal of making their mobile platforms attractive to app developers. One way they did this was to make a core set of user data from the smartphone available to third party developers to use in their apps, in order to encourage developers to create apps that were useful and personalizable for

customers. This data included location data, which originally was available to any app an individual downloaded on their smartphone. This meant that any app could obtain some form of location data from an individual user without asking specific permission in real time. As I will discuss in more detail below, “permission” with respect to third party apps was assumed to be granted by the user’s decision to download and install the app. Default location access created an ecosystem where app developers were able to access, without asking the user directly, a set of data that was far more personal than anything they could have obtained through a traditional browser-based website.

2. Mobile Permissions

When Android users sought to download an app, either through the Google Play store or directly from a website, prior to installation they were presented with a list of permissions that the app required in order to function. Known as “install-time permissions,” this list was intended to provide users with a notice of the types of data the app would request from their phone. However, many of these permissions used technical descriptions that non-technical people did not understand, making permissions lists incomprehensible to the average consumer.¹⁸³ Furthermore, prior to 2015, users could not deny any of these permissions; they had to accept them all or decide not to download the app, operating under the same take-it-or-leave-it terms as other online services. A user could not tell an app with no functional use for their location not to access this data unless they turned off location services on the phone, which would then deny

¹⁸³ See generally: Jennifer King. *How Come I’m Allowing Strangers To Go Through My Phone? Smartphones and Privacy Expectations*. Workshop on Usable Privacy and Security for Mobile Devices (U-PriSM) at SOUPS, July 2012. Washington, D.C., USA; Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. 2012. Android permissions: user attention, comprehension, and behavior. In Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS '12). Association for Computing Machinery, New York, NY, USA, Article 3, 1–14.

location to all apps on the phone. However, doing so could also cause apps that expected access to permission by default to crash and become inoperable.

Android version 6.0 (Marshmallow), released in 2015, changed all-or-nothing permissions with the introduction of a runtime permission model. After this update, apps needed to request “dangerous” permissions—including location access—at the moment the app required them for a certain functionality, rather than at the time of installation.¹⁸⁴ This change forced developers to present permissions, accompanied by a description of why they were needed, in context.

Android app permissions, however, do not fundamentally address the issue of whether users understand when and how often their location data is being collected, including by the operating system itself. The install-time permissions model, which requires agreement to a privacy policy and to an app’s permissions at a discrete moment in time, does not foretell what one’s actual experience will be with using the app or service over time. What can be especially difficult to understand at installation is the long-term experience with using a mobile app: how often personal data is recorded, how long it is kept, and whether it is used outside of the context in which it was originally collected. Even with the runtime permissions model, which presents real-time notifications and requests for location access, it is still difficult for users to understand how data is being collected in the aggregate. And none of these permission models explain to users precisely how their data might be used outside of the instant purpose for which it was collected.

Further, as explained above, one of the allegations against Google here is that it does not necessarily honor runtime permission settings. Apps that are denied location run-time permissions are still able to obtain location data from the user from *other* apps that are granted

¹⁸⁴ <https://android-developers.googleblog.com/2015/08/building-better-apps-with-runtime.html>

permission.¹⁸⁵ Internal Google documents discussing (i) “the problem re: Google apps sharing location information in the backend without honoring the app permission on device”; (ii) the fact that apps “exchange data on the backend without enforcing running permissions”; (iii) that

[REDACTED]

[REDACTED]; (iv) that [REDACTED]

[REDACTED]¹⁸⁶ Dr. Nielson further confirmed this point in his declaration, as discussed above. Users have no ability to avoid harms if users do not know about them.

The same is true with respect to the other wrongful conduct alleged here. For example, not only are users unable to “opt out” of IPGeo and [REDACTED], they do not know about these services. Relatedly, when users disable their device location, they have no way to prevent (or even know about) Google’s “off means course” decision. As another example, the Complaint (at paragraphs 110-112) further alleges that Google modified its user interface to minimize opportunities for uses to disable locations, and that it persuaded its Android partners to do so same. Above, I also explained how difficult it would be for Android users to avoid using a Google Account with their phone, even if they want to avoid sending location data to Google. Similarly, finding the relevant settings that would stop location tracking is not only elusive but ultimately does not stop the tracking. Preventing Google from inferring a users’ home or work location requires the user to set an inaccurate one—something users do not know about. Users cannot reasonably avoid these harms.

¹⁸⁵ Complaint ¶¶81-86; Nielson 11/16/2021 ¶¶ 90-97.

¹⁸⁶ Complaint ¶81 and cited documents in that paragraph.

3. Design Didn't Match People's Expectations or Desires

Both at Google and within the larger industry, there has been evidence for some time now that the design of these location features does not match what users expect or want. In 2012, researchers at UC Berkeley published a nationally representative survey report of 1200 U.S. residents exploring their privacy expectations regarding mobile phones (including smartphones). According to the report, “A large majority—78%—of Americans consider information on their mobile phones at least as private as that on their home computers. Fifty-nine percent consider it “about as private” and 19% consider it “more private.”¹⁸⁷ The survey also asked two questions about location tracking; first, how long cell phone providers should keep a history of a subscriber's location. According to the survey, “[a] plurality of respondents—46%—answered that wireless phone location data should not be kept at all (this option was offered to respondents after all the other periods of retention). The next largest group—28% of respondents—answered that the data should be kept less than a year.”¹⁸⁸ When asked if they wanted their cell providers to use their location data for targeted advertisements, “92% of respondents said that they would “definitely” or “probably” not allow the use of location data for this purpose.”¹⁸⁹ My own research¹⁹⁰ conducted in the same time frame as this survey supported these findings: smartphone users had significant concerns about the use of their personal data, including location data, on their smartphones. However, those concerns were not being respected in the design of these devices, from the system architecture to the user interface.

¹⁸⁷ Urban, Jennifer M. and Hoofnagle, Chris Jay and Li, Su. Mobile Phones and Privacy (July 10, 2012). BCLT Research Paper Series, UC Berkeley Public Law Research Paper No. 2103405, p.9

¹⁸⁸ Ibid., p.19.

¹⁸⁹ Ibid.

¹⁹⁰ Jennifer King. How Come I'm Allowing Strangers To Go Through My Phone? Smartphones and Privacy Expectations. Workshop on Usable Privacy and Security for Mobile Devices (U-PriSM) at SOUPS, July 2012. Washington, D.C., USA.

Other studies have corroborated the conclusion that users' privacy wishes are not being met. Users have enormously rich location privacy preferences.¹⁹¹ Timing and setting are chief among these preferences. Users care greatly about when and with what frequency their location data is collected.¹⁹² Furthermore, users are more comfortable both sharing¹⁹³ and selling¹⁹⁴ location in more public settings, such as work and public transit, than their own home, which is visited by a smaller and less diverse set of people. In addition, location data can also reveal a wide array of information about a user's interests, beliefs, and characteristics.¹⁹⁵ Users care to protect some of these secondary data points, such as health and socioeconomic status, with much more privacy than others, such as the user's skillset.¹⁹⁶

As discussed above, the State alleges (and Google's internal documents show) that Google knows users do not understand the settings. They also show that the settings do not match their expectations. Google's internal documents (discussed above) suggest that users expect that disabling "location history" would not mean that Google continues to collect and

¹⁹¹ Michael Benisch, Patrick Gage Kelley, Norman Sadeh, and Lorrie Faith Cranor, "Capturing Location-Privacy Preferences: Quantifying Accuracy and User-Burden Tradeoffs," *Personal and Ubiquitous Computing* 15, no. 7 (October 2011): 679-94.

¹⁹² Bart P. Knijnenburg, Alfred Kobsa, and Hongxia Jin, "Preference-based location sharing: are more privacy options really better?" *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '13)* (New York: Association for Computing Machinery, 2013): 2667-76, <https://dl.acm.org/doi/pdf/10.1145/2470654.2481369>; Benisch et al., *supra* note 191.

¹⁹³ Eran Toch, Justin Cranshaw, Paul Hanks Drielsma, Janice Y. Tsai, Patrick Gage Kelley, James Springfield, Lorrie Cranor, Jason Hong, and Norman Sadeh, "Empirical models of privacy in location sharing," *Proceedings of the 12th ACM international conference on Ubiquitous computing (UbiComp '10)* (New York: Association for Computing Machinery, 2010): 129-38, <https://dl.acm.org/doi/pdf/10.1145/1864349.1864364>.

¹⁹⁴ Omer Barak, Gabriella Cohen, Alla Gazit, and Eran, "The price is right? Economic value of location sharing," *Proceedings of the 2013 ACM Conference on Pervasive and Ubiquitous Computing Adjunct Publication (UbiComp '13 Adjunct)* (New York: Association for Computing Machinery, 2013): 891-900, <https://dl.acm.org/doi/pdf/10.1145/2494091.2497343>.

¹⁹⁵ Benjamin Baron and Mirco Musolesi, "Where You Go Matters: A Study on the Privacy Implications of Continuous Location Tracking," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 4, no. 4 (December 2020): Article No. 169, 1-32, <https://dl.acm.org/doi/pdf/10.1145/3432699>.

¹⁹⁶ *Ibid.*

store location. Also, as discussed above, after the AP Article, Senator Blumenthal tweeted: “It should be simple—‘off’ mean ‘off.’” Instead, after the AP Article, Google implemented “off means course.”¹⁹⁷

Users cannot avoid undesirable location tracking, but mobile OS developers certainly can. Designing to cater to privacy preferences is far from an impossible task. In fact, as early as 2010, researchers were discussing the risks of, and potential solutions to, personalization technologies that individualize advertisements or experiences based on users’ locations, search histories, or demographic information.¹⁹⁸ Personalizing location privacy settings offers one possible response: allowing users to take greater control of their location data, in part to address the “intrusive”¹⁹⁹ nature of personalization technologies.

4. The Power of Defaults

Default settings can be convenient for users (allowing you to save your preferences rather than having to reset them every time you use a device or service), but it is a well-established design principle that defaults are “sticky”—meaning, once they are set, users rarely change them. Accordingly, if on a mobile device all of the components that allow for location tracking (GPS, Wi-Fi, Bluetooth, internet data) are on by default, and any settings that allow the user to restrict these data flows are also enabled by default, the majority of users are unlikely to change them, creating a situation where a user must opt-out of data collection, rather than opt-in. Furthermore, if these various settings and controls take effort or are difficult to locate on a device, or as in the case of Google’s Web & App activity (which controls location collection while using Google

¹⁹⁷ GOOG-GLAZ-00001422 at 1428.

¹⁹⁸ Eran Toch, Yang Wang, and Lorrie F. Cranor, “Personalization and Privacy: A Survey of Privacy Risks and Remedies in Personalization-Based Systems,” *User Modeling and User-Adapted Interaction* 22 (March 2012): 203-20.

¹⁹⁹ Awad and Krishnan 2006, cited at 214 of TWC.

services and products) are not even clearly tied to location, then navigating across all of these settings, understanding how they all interact, and remembering what state they are in (on or off) can be extremely complex for many users.

Adding to this complexity is the ease or difficulty with which users are able to make choices on a per-app basis (e.g., deciding to allow location access to a ride-sharing app, but not to a banking app), how “sticky” those choices are, and whether the smartphone’s operating system provides prompts or nudges to help the user understand when their location is being used and why. Otherwise, if the default state on a smartphone is “opt-out” for all of these forms of data or requires setting privacy preferences, the default state a user can find themselves in is one where their location data is being collected.

The danger of Google’s location defaults has not gone unnoticed. In 2019, the Australian Competition and Consumer Commission (ACCC) sued Google for deceptive location data collection practices.²⁰⁰ By burying user consent toggles under a series of unclear settings categories—including Bluetooth, WiFi, and “Web and App Activity”—Google was able to conceal its default of data collection from users. In finding for the ACCC, the Australian Federal Court emphasized that reasonable users would be misled into thinking they controlled location data that they in fact did not.²⁰¹ Particularly because Google has acknowledged the sensitivity of location data when held by other collectors, the opt-out nature of some of Google’s collection practices indicates a dangerous willingness to place the large burden of data protection on poorly informed consumers.²⁰²

²⁰⁰ ACCC v Google Order, AZAG-0000001.

²⁰¹ <https://www.accc.gov.au/system/files/ACCC%20v%20Google%20LLC%20-%20Concise%20Statement.pdf>; *see also*

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3973199.

²⁰² MarloJMcGriffIIPMKGoogle pg 60.

The impact of defaults on Google’s location data collection extends beyond Android devices. As I discussed above, one way Google creates greater location accuracy is by building out a proprietary database of WiFi access points (WAPs) that includes information about the WAPs’ location. These access points share their information with Google by default.²⁰³ If Wi-Fi location tracking is enabled, as it is by default on Android devices, users’ phones send the details of nearby Wi-Fi networks to the database, too. Mobile devices and routers thus create a crowdsourced mass of location, device, and Wi-Fi data that Google is able to swallow in gulps.

Of course, these concerns are even more “unavailable” where opting out as not an option. For example, as noted above, based on my review of Dr. Nielson’s declaration, users can’t even opt out of some location collection, e.g., from IPGeo).

VII. GOOGLE’S PROPOSED JUSTIFICATIONS DO NOT OUTWEIGH THESE HARMS

Against the allegations leveled by the State, I understand Google contends that “its location services and technologies provide significant benefits to users of its services, whether consumers or business, and provide public and competitive benefit as well. Google offers granular location controls to users and strives to make sure its products and services are well understood, including through its clear and detailed disclosures.”

The harms (or injuries) from Google’s systematic collection and storage of consumer location data are not outweighed by countervailing benefits. At a general level, the benefits of continuous location tracking are heavily skewed in favor of the trackers, not consumers. The inherent unfairness of systematic location tracking, built upon ever growing information

²⁰³ <https://support.google.com/maps/answer/1725632?hl=en#zippy=%2Chow-do-i-opt-my-access-point-out-of-google-location-services> - describing an opt-out process; see also whitepaper 64.

asymmetries between individual consumers and the companies that track them, mean that in exchange for access in real-time to a location dependent service, consumers “pay” by handing over information detailing their every move. But the biggest benefit goes to the collectors of this data themselves as they monetize it in ways that far exceed the context for which it was collected.²⁰⁴ Thus, consumers end up paying for location-based free services not only by handing over personal data that exceeds the scope of the request, but by having their personal data used without their consent in ways that can actually cause them harm.

While smartphones represent an incredible leap forward for both telephony and mobile computing compared to their predecessors, their ability to provide accurate, real-time location data in particular was a paradigm shift. Knowing your real-time precise location was useful for personal wayfinding using a mapping application; suddenly, even unfamiliar places became navigable without a paper map. But this level of precision was also a boon for businesses. Even a general idea of where a smartphone user was located in real time offered a degree of contextual knowledge to software developers that could improve the utility of many applications, as well as to the advertisers that wanted to serve people ads.

That said, the allegations in this case go beyond just “systematic collection and storage of consumer location data.” The conduct challenged here by the State of Arizona (and recognized by multiple Google employees and officers themselves) is that Google offers the illusion of choice when, in fact, no such choice is available. There is no opt-out from Google’s collection, storage and use of location data through IPGeo or [REDACTED]. For the device location, the State alleges that Google deliberately moved the setting in order to minimize users’ ability to disable it. Even when device location is off, Google interprets that as a license to collect coarsened data. The allegations are that Google continues to collect location data through

²⁰⁴ See generally: Hoofnagle & Whittington, *supra* note 178.

“WAA” even when the “Location History” is off. Google is also collecting and storing far more data and holding onto it far longer than is actually necessary to provide services to consumers.

The conclusion that the benefits do not outweigh the harms is bolstered by Google’s own admission that “*one of the most sensitive and vast personal signals that we collect from users is User Location.*”²⁰⁵

It is my understanding that Google disputes some (although not all) of these allegations. But assuming the jury agrees with them, I have not seen Google offer any benefits for this conduct, much less ones that outweighed by countervailing factors.

VIII. CONCLUSION

Despite the complexity and the amount of data collected about us today, people still continue to demand greater privacy rights and control. Survey data over the past decade and more consistently demonstrates a strong belief and desire by the public in the need for companies to respect their data privacy.²⁰⁶ The primary reason individuals continue to use smartphones and other products and services that collect data is that, until recently, there were few companies that

²⁰⁵ GOOG-GLAZ-00317865 at p. 4 (emphasis added). David Monsees, a Google product manager, agreed in testimony before the Federal Court of Australia in *Australian Competition and Consumer Commission v. Google*, 2021 FCA 367 (NSD 1760 of 2019), that the location data generated by WAA is used to geo-target ads, and later agreed that location is “one of the most sensitive and vast personal signals we collect from users.” Ex. 9, GOOG-GLAZ-00299120, at 169; *ibid.* at 137 (admitting that WAA tracks user location for ads service).

²⁰⁶ *See generally*: Brooke Auxier *et al.* “Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information.” Pew Research Center, Nov. 15, 2019. <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/>; Lee Rainie and Maeve Duggan. “Privacy and Information Sharing.” Pew Research Center, Jan. 14, 2016. <https://www.pewresearch.org/internet/2016/01/14/privacy-and-information-sharing/>; Mary Madden and Lee Rainie. “Americans’ Attitudes About Privacy, Security and Surveillance”. Pew Research Center, May 20, 2015. <https://www.pewresearch.org/internet/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/>. Mary Madden. “Public Perceptions of Privacy and Security in the Post-Snowden Era” Pew Research Center, Nov. 12, 2014. <https://www.pewresearch.org/internet/2014/11/12/public-privacy-perceptions/>.

competed on the basis of privacy. Further, the fact that the vast majority of companies offer non-negotiable, take-it-or-leave-it terms can make “choice” a challenging concept. In 2014, reporter Julia Angwin documented in her book, *Dragnet Nation*, the year she spent trying to live without being tracked by technology.²⁰⁷ Suffice to say it practically required that she leave the modern world. Given how many facets of our lives today require a computer to use, including many public services and benefits, the argument that if people truly cared about privacy that they would simply stop using smartphones and other devices and services is simply fictional.

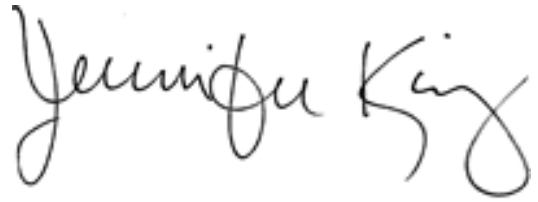
Finally, location privacy is important because data privacy ensures the autonomy that is central to democracy. Giving users the opportunity to meaningfully consent to location tracking allows users to understand when and how their sensitive personal information will be used to predict and ultimately influence their future behavior. Absent privacy, individuals become unwittingly subject to micro-targeting that can shape their purchases, information ingestion, and social circles into unrepresentative fragments of society. Democracy hinges on our free and informed choice. Our choices around location tracking are, by nature, made under constraint and in ignorance. Without privacy and the freedom to exert our autonomy, the foundation of our democracy is put at risk.

To restate my conclusions, it is my opinion that Google’s systematic collection and storage of consumers’ personal location data causes substantial injury to consumers that they cannot reasonably avoid. This is particularly true, given the manner in which Google accomplishes this, as discussed above. These harms resulting to consumers are not outweighed by countervailing benefits to consumers or to competition for the reasons explained above.

²⁰⁷ Julia Angwin. *Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance* (Times Books, 2014).

May 4, 2022

Berkeley, CA

A handwritten signature in black ink that reads "Jennifer King". The signature is written in a cursive style with a large, looping "J" and "K".

Jennifer King, Ph.D.

Appendix 1: Case-Related Documents Reviewed

1. The ACCC v. Google Order, AZAG-000001.
2. The Every Step You Take report
3. A.R.S. 44-1521, available at
<https://www.azleg.gov/viewdocument/?docName=https://www.azleg.gov/ars/44/01521.htm>
4. A.R.S. 44-1522, available at
<https://www.azleg.gov/viewdocument/?docName=https://www.azleg.gov/ars/44/01522.htm>
5. The Deceived by Design Report of the Norwegian Consumer Council
6. The complaint and exhibits in this matter.
7. The redacted declaration of Pablo Camacho.
8. Douglas C. Schmidt, Google Data Collection (2018).
9. Google’s Motion for Summary Judgment.
10. Redacted version of the State’s CSOF.
11. Seth Neilson’s 11/16/2021 Declaration
12. Redacted version of State’s response to Google’s MSJ
13. Redacted version of State’s SSOF
14. Google’s Reply In Support of Summary Judgment
15. The Oracle White Paper (Google, Android, the End of Notice-and-Choice),
16. Judge Thomason’s order on Google’s MSJ (redacted)
17. AP News Article <https://apnews.com/article/north-america-science-technology-business-ap-top-news-828aefab64d4411bac257a07c1af0ecb>
18. New York Times 2019 Report,
<https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html>

19. GOOG-GLAZ-00001371
20. GOOG-GLAZ-00001521
21. GOOG-GLAZ-00222226
22. GOOG-GLAZ-00224887
23. GOOG-GLAZ-00283334
24. GOOG-GLAZ-00315032
25. GOOG-GLAZ-00001422
26. GOOG-GLAZ-00002914
27. GOOG-GLAZ-00274982
28. GOOG-GLAZ-00299120
29. GOOG-GLAZ-00312666
30. GOOG-GLAZ-00317865

Exhibit A

Jennifer King, Ph.D

1511 Cedar St.
Berkeley, CA 94703

jen@jenking.net

www.jenking.net

415-990-8227

Academic Appointments

Privacy and Data Policy Fellow, Stanford Institute for Human Centered Artificial Intelligence Jan. 2021-present

At HAI I conduct information privacy research with a specific focus on artificial intelligence, as well as work with Professors Sarah Billington and James Landay on a research project examining the impact of sensors used in workplace environments to promote health and well-being. In this role I also engage with and advise policymakers, legislators, and governmental entities on issues related to information privacy, as well as collaborate with HAI colleagues on promoting interdisciplinary policy-focused research at Stanford.

Director of Consumer Privacy, Center for Internet and Society, Stanford Law School April 2018-Dec. 2020

In this role I conducted privacy-focused research in the public interest on topics such as genetic privacy, the Internet of Things, notice and consent, and artificial intelligence. I actively participated in the management of the Center, including strategic planning for research and fundraising. I also engaged with and advise policymakers, legislators, and governmental entities on issues related to information privacy.

Degrees

University of California, Berkeley School of Information

Ph.D, Information Management and Systems

2009 – May 2018

- My dissertation, "Privacy and Social Exchange Theory," used a social relational framework to explore consumer motivations for disclosing personal information to companies. I employed both qualitative and experimental methods for this research. It was selected as the runner up in the Information Schools (I-Schools) Organization's 2019 Best Dissertation Award. Dissertation advisors: Deirdre Mulligan, Coye Cheshire, Steve Weber, and David Wagner.
- Focus areas: human-computer interaction, social computing, and information law and policy.
- Research funded by grants from the Center for Long Term Cybersecurity (inaugural grantee), the National Science Foundation through TRUST (Team for Research Through Ubiquitous Secure Technology) and the I3P (Institute for Information Infrastructure Protection).
- Co-director of the student led Center for Technology, Society & Policy for the 2016-2017 academic year. CTSP funds fellows and projects, organizes events, and hosts speakers supporting our four focus areas: engineering ethics, digital citizenship, evaluating technology policy, and supporting future technologists.

University of California, Berkeley, Masters of Information Management and Systems (MIMS)

2006

University of California, Irvine

1994

- Bachelor of Arts, Political Science and Sociology with Honors in Political Science.
- Admission with Distinction, Campuswide Honors Program, National Political Science Honors Society, National Sociology Honors Society, Dean's List, UCDC Scholarship Award Recipient, Lyndon B. Johnson Congressional Fellow.

Peer Reviewed Journal and Conference Publications

Mulligan, D.K., Regan, P.M. and **King, J.** (2020), The Fertile Dark Matter of Privacy takes on the Dark Patterns of Surveillance. *J. Consum. Psychol.*, 30: 767-773. <https://doi-org/10.1002/jcpy.1190>

Jennifer King. 2019. "Becoming Part of Something Bigger": Direct to Consumer Genetic Testing, Privacy, and Personal Disclosure. Proc. ACM Hum.-Comput. Interact. 3, CSCW, Article 158 (November 2019), 33 pages. <https://doi.org/10.1145/3359260>

Christopher Thompson, Maritza Johnson, Serge Egelman, David Wagner, and **Jennifer King**. "When It's Better to Ask Forgiveness than Get Permission: Attribution Mechanisms for Smartphone Resources." Presented at the Symposium on Usable Privacy and Security, July 2013. Newcastle, UK.

Jennifer King, Airi Lampinen, and Alex Smolen. "Privacy: Is There An App For That?" Presented at the Symposium on Usable Privacy and Security, July 2011. Pittsburgh, PA.

King, Jennifer and Selcugoklu, Aylin. "Where's the Beep? User Misunderstandings of RFID." In Proceedings of 2011 IEEE International Conference on RFID.

M. Meingast, **J. King**, D. Mulligan. "Embedded RFID and Everyday Things: A Case Study of the Security and Privacy Risks of the U.S. e-Passport." In Proceedings of IEEE International Conference on RFID, March 2007.

M. Meingast, **J. King**, D. Mulligan. "Security and Privacy Risks of Embedded RFID in Everyday Things: the e-Passport and Beyond," *Journal of Communications*, 2(7), 2007.

Law Review Articles and Refereed Workshop Publications

Jennifer King and Adriana Stephan. Regulating Dark Patterns in Practice – Applying the California Privacy Rights Act. Georgetown Technology and Law Review. 5 Geo. L. Tech. Rev. 251 (2021).

Jennifer King, Richmond Wong, Rena Coen, Jael Makagon, and Andreas Katsanevas. "This All Seemed Fairly Normal To Me"—The Absence of Effect of Privacy Policy Links on Invasive Personal Disclosure. Presented at the Privacy Law Scholars Conference (invitation only), May 2019, Berkeley, CA.

Jennifer King, "Privacy, Disclosure, and Social Exchange Theory." UC Berkeley dissertation, filed May 2018. A draft of this work was presented at the Privacy Law Scholars Conference (invitation only), June 2015, Berkeley, CA.

Jennifer King, "Understanding Privacy Decision-Making Using Social Exchange Theory." Presented at The Future of Networked Privacy: Challenges and Opportunities workshop, CSCW March 2015.

Jennifer King. "Taken Out of Context: An Empirical Analysis of Westin's Privacy Scale." Presented at the Workshop on Privacy Personas and Segmentation (PPS) at SOUPS, July 2014. Menlo Park, CA, USA.

Deirdre K. Mulligan and **Jennifer King**. "Bridging the Gap Between Privacy and Design." University of Pennsylvania Journal of Constitutional Law, Vol. 14, Issue 4, 2012. Selected as a Leading Paper for Policymakers by the Future of Privacy Forum, 2012.

Jennifer King. "How Come I'm Allowing Strangers To Go Through My Phone?: Smartphones And Privacy Expectations." Presented at the Workshop on Usable Privacy and Security for Mobile Devices (U-PriSM) at SOUPS, July 2012. Washington, D.C., USA. Note: This paper was also presented at the Privacy Law Scholars Conference (invitation only), June 2012, Washington, D.C., USA. Selected as a Leading Paper for Policymakers by the Future of Privacy Forum, 2012.

Jennifer King and Deirdre K. Mulligan. "Reconceptualizing Privacy for Social Media Research and Design." Presented at *Reconciling Privacy with Social Media* workshop, CSCW, 2012.

Jennifer King and Andrew McDiarmid. "Where's The Beep? Security, Privacy, and User Misunderstandings of RFID." In proceedings of USENIX Usability, Security, and Psychology. San Francisco, CA, April 14, 2008. Available at: <http://portal.acm.org/citation.cfm?id=1387652>

Egelman, Serge, **King, Jen**, Miller, Robert C., Ragouzis, Nick, and Shehan, Erika. "Security User Studies: Methodologies and Best Practices." Extended abstracts of the ACM Conference on Human Factors in Computing Systems (CHI 2007). San Jose, CA, USA, April 28, 2007.

Research Reports and White Papers

Daniel Ho, **Jennifer King**, Russell Wald, and Chris Wan. Building A National AI Research Resource: A Blueprint for A National Research Cloud. White Paper: Stanford Institute for Human-Centered Artificial Intelligence, October 2021. Available at: <https://hai.stanford.edu/policy/national-research-cloud>

King, Jennifer; Flanagan, Anne; Warren, Sheila. Redesigning Data Privacy: Reimagining Notice & Consent for Human-Technology Interaction. White paper report: World Economic Forum, 30 July 2020. Available at: <https://www.weforum.org/reports/redesigning-data-privacy-reimagining-notice-consent-for-humantechnology-interaction>.

Hoofnagle, Chris; **King, Jennifer**; Li, Su; and Turow, Joseph. "How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies?" April 14, 2010. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864. Selected as a Leading Paper for Policymakers by the Future of Privacy Forum, 2010.

Turow, Joseph; **King, Jennifer**; Hoofnagle, Chris; Bleakley, Amy; and Hennessey, Michael. "Americans Reject Tailored Advertising and the Three Activities That Enable It." September 29, 2009. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214

Jennifer King, Deirdre Mulligan, and Steven Raphael. "CITRIS Report: An Evaluation of the Effectiveness of the City of San Francisco's Community Safety Cameras." Presented before the City of San Francisco Police Commission, January 2009.

Chris Jay Hoofnagle and **Jennifer King**. "Research Report: What Californians Understand About Privacy Online." September 3, 2008. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1262130

Chris Jay Hoofnagle and **Jennifer King**. "Research Report: What Californians Understand About Privacy Offline." May 15, 2008. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1133075

Jennifer King and Chris Jay Hoofnagle, "A Supermajority of Californians Support Limits on Law Enforcement Access to Cell Phone Location Information," February 2008. Presented at the 37th Research Conference on Communication, Information and Internet Policy (TPRC), September 26, 2008, George Mason University, Alexandria, VA. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1137988

Chris Jay Hoofnagle and **Jennifer King**. "Consumer Information Sharing: Where The Sun Still Don't Shine," December 2007. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1137990

Op-Eds and Popular Press

Jennifer King. "[Opinion: After Rape Survivor's Arrest, It's Time To Rethink Genetic Databases.](#)" *The Washington Post*, Feb. 17, 2022.

Jennifer King and Jael Makagon. "[The fallacy behind private surveillance cameras in San Francisco.](#)" *Cal Matters*, August 9, 2020.

Jen King. "[Change your phone settings so Apple, Google can't track your movements.](#)" *The Conversation*, Jan. 14, 2019.

Invited Talks & Panels

Regulating Artificial Intelligence Through Data Protection. [Global Privacy Assembly](#), Keynote Speaker, October 18, 2021.

[Bringing Dark Patterns To Light—An FTC Workshop](#). Panelist, April 29, 2021.

[Dark Patterns, Icons and Toggles: A Conversation on Design and Regulation](#). IAPP Global Summit, April 23, 2021. (panelist)

[Dark Patterns: Manipulative UX Design and the Role of Regulation](#). Future of Privacy Forum, March 24, 2021. (main presenter)

[The Rise of Trust Brokers](#). World Economic Forum Sustainable Development Impact Summit, Sept. 24, 2020.

"[Notice, Consent, and Disclosure in Times of Crisis](#)." Atlantic Council Data Salon Series, May 27, 2020. (main presenter)

"Integrating Privacy, Personal Disclosure, and Social Exchange Theory: An Experimental Test." [Ostrom Workshop Colloquium](#), Indiana University, Bloomington, IN, October 21, 2019. (main presenter)

[The Trust Paradox: The Future of Privacy and Transparency in the Digital Economy](#). The Churchill Club, San Mateo, CA, March 29, 2019 (panelist).

"The Cambridge Analytica Debacle," International Association of Defense Counsel, Santa Barbara, CA, February 27, 2019.

"Privacy, Anonymity, and Consent." [Conference On Mobile Position Awareness Systems and Solutions](#), San Francisco, CA, Sept. 7, 2018.

Data Privacy Day (panel), World Economic Forum Center for the Fourth Industrial Revolution, San Francisco, CA, June 5, 2018.

[Designing Trustable Products: Microinteractions Matter For Secure UX](#) (panel). O'Reilly Design Conference, March 22, 2017.

Security & Human Behavior, Harvard Law School, May 2016.

TRUSTe Internet of Things Privacy Summit, June 17, 2015. Panelist, "Enabling Smart Cities: Planning for Privacy."

In Short – Advertising and Privacy Disclosures for a Digital World. Federal Trade Commission workshop, May 30, 2012. – Opening speaker and panelist.

How To Personalize Without Being Creepy. SXSW Interactive – March 14, 2011. Austin, TX. – Panelist.

“A Supermajority of Californians Support Limits on Law Enforcement Access to Cell Phone Location Information,” given at the 37th Research Conference on Communication, Information and Internet Policy (TPRC), September 26, 2008, George Mason University, Alexandria, VA.

“Where’s the Beep? Security, Privacy, and User Misunderstandings of RFID,” given at “Pay On The Go: Consumers and Contactless Payment,” Federal Trade Commission Town Hall Meeting, July 24, 2008, University of Washington, Seattle, WA. – Panelist.

“The State of CCTV in the United States,” given at the 3rd Annual Surveillance and Society Conference “InVisibilities: The Practice and Experience of Surveillance in Everyday Life,” April 3, 2008, University of Sheffield, Sheffield, England, UK.

“CCTV: Developing Privacy Best Practices,” Department of Homeland Security Workshop, December 17-18, 2007, Alexandria, VA. – Panelist

“Sensors as Disruptive Technology: Guidelines for Future Development,” given at the IBM Sensor Day, October 2007, UC Berkeley, Berkeley, CA.

“Embedded RFID and Everyday Things: A Case Study of the Security and Privacy Risks of the U.S. e-Passport,” given at the IEEE International Conference on RFID, March 2007, Grapevine, TX.

“RFID: A Case Study of the Risks and Benefits of Location-Aware Technologies,” given at the O’Reilly Emerging Technology Conference, March 8, 2006, San Diego, CA.

Teaching Experience

Co-instructor (with Professor Dan Ho), Law 807Z: Creating a National Research Cloud, Policy Practicum, Winter-Spring 2021, Stanford Law School.

Co-Instructor (with Professor Coye Cheshire), I216: Computer Mediated Communication (graduate level course). Fall 2016, Spring 2016, U.C. Berkeley School of Information.

Sponsored Research

Co-PI: CNS Core: **Large: Autonomy and Privacy with Open Federated Virtual Assistants**, National Science Foundation, Award RSGA-1900638, PI Monica S. Lam, Co-PIs Chris Re; Christopher Manning; Dan Boneh; David Mazieres; James Landay; Michael Bernstein, April ‘19-Sept. ‘23, Stanford University: \$627,077.

PI: **Exploring User Perceptions of Personal Data Ownership and Management**. 2019 H2 Mozilla Research Projects Grant, Stanford Center for Internet and Society, Jan.-Dec. ‘20, \$40,000.

Awards, Honors and Service

Awards:

Best Dissertation Award, Runner-Up: Information Schools (I-Schools) Organization, 2019

Selected leading paper, Future of Privacy Forum's Annual Privacy Papers for Policy Makers Award, 2012 (two papers) and 2010. *This Award recognizes leading privacy scholarship that is relevant to policymakers in the United States Congress, at U.S. federal agencies and for data protection authorities abroad.*

UC Berkeley School of Information Dr. James R. Chen Award for Outstanding Master's Final Project "Social Uses of Communication Backchannels in a Shared Physical Space," 2006.

Public Service:

Committee Member, California State Advisory Board on Mobile Privacy Policies, 2012

Member, State of California RFID Advisory Board, 10.07 – 3.08

Leadership Roles (Conferences and Workshops):

Program Committee, *Symposium on Usable Privacy and Security*, 2020

Organizer, *Redesigning Consent for Better Data Protection*, Oct. 2-3, 2019. Co-hosted with the World Economic Forum Center for the Fourth Industrial Revolution, San Francisco, CA

Program Organizer, *Workshop on Privacy Indicators and The Future of Privacy Indicators Workshop*, SOUPS, June 2016

Program Organizer, *Bridging the Gap Between Privacy by Design and Privacy in Practice*, CHI, May 2016

Program Organizer, *Privacy By Design: Privacy Enabling Design*, Computing Community Consortium, May 2015

Program Organizer, *Security User Studies: Methodologies and Best Practices*, CHI Workshop, 2007

Committee Member, *Privacy & Power: Acknowledging the Importance of Privacy Design for Vulnerable Populations*, CHI Workshop, 2020

Committee Member, *Ubiquitous Privacy: Research and Design for Mobile and IoT Platforms*, CSCW Workshop, 2019

Committee Member, *The Future of Networked Privacy: Challenges and Opportunities*, CSCW Workshop, 2015

Committee Member, *Measuring Networked Privacy*, CSCW Workshop, 2013

Conference & Journal Reviewing:

CSCW: 2019, 2017, 2016, 2015, 2013

International Workshop on Privacy Engineering – IWPE 2016

CHI: 2021, 2020, 2019, 2018, 2014

IEEE RFID 2012

External Consulting

Contract Litigation Consultant/Expert Witness

2010 – Present

I provide expert services to clients (Federal Trade Commission, Federal Reserve Board, State of Washington, City of Santa Monica, City of Santa Cruz, and others) focusing on online disclosures, negative option continuity programs, online credibility, deception, dark patterns, and general website usability issues.

Major Cases include:

- Testifying Expert, *FTC vs. Amazon (2:14-cv-01038-JCC)*. I completed an expert report, rebuttal report, and was deposed. My expert report provided a heuristic analysis of the in-app purchase process as well as an analysis of thousands of customer complaints. The case was decided on summary judgment in favor of the FTC, finding Amazon liable for unauthorized in-app purchases by children on the Kindle Fire tablet.
- Testifying Expert, *FTC vs. Commerce Planet (8:09-cv-01324-CJC(RNBx))*. I completed an expert report, rebuttal report, was deposed, and testified at trial. The substance of my report was a heuristic evaluation of a portion of the Commerce Planet website to determine the clarity and conspicuousness of negative option marketing disclosures to consumers. The case resulted in a permanent injunction, restitution, and disgorgement against the defendant for deceptive and unfair practices violating Section 5(a) of the FTC Act.

Previous Professional Experience

Prior to beginning my Ph.D program, I was a Research Specialist at the Samuelson Law, Technology, and Public Policy Clinic at U.C. Berkeley Law (2007-2009). My earlier professional career was as a product manager in the online software industry over a period of seven years, most notably at Yahoo!.