The spy in our pockets

How location tracking is raising the stakes on privacy protection

EY
Building a better working world

Authors:

Meribeth Banaschik

Partner, Forensic & Integrity Services
Ernst & Young GmbH
Wirtschaftsprüfungsgesellschaft
Germany

Kristina Miggiani

Senior Manager, Forensic & Integrity Services
Ernst & Young GmbH
Wirtschaftsprüfungsgesellschaft
Germany

Introduction

Our attachment to smartphones has made them the perfect devices to track our movements – providing invaluable data to businesses and governments. Little do we know that many apps on our phones allow location data companies to pinpoint how we spend our days. A *New York Times* investigation was able to use a data set to track the movements of individuals commuting to their offices, picking up their children at school and even breaking their routines to go on a job interview.[1]

Rising concern over location tracking is just one example of how protecting privacy is becoming increasingly complex. COVID-19 is exacerbating the issue as governments and businesses experiment with new technologies to track and contain the outbreak. These efforts are saving lives, but they also raise fears about intruding on privacy and exposing personal health data.

Privacy management is often seen as the responsibility of compliance and legal professionals, aided by the cybersecurity team. But more and more organizations are realizing that privacy is impacting stakeholders in just about every corner of the organization. Managing privacy risk brought on by location tracking requires a concerted effort that also includes human resources, operations, information security, communications and investor relations.

[1] Stuart A. Thompson and Charlie Warzel, "Twelve Million Phones, One Dataset, Zero Privacy," *The New York Times*, 19 December 2019, www.nytimes.com.

Privacy claims for location tracking subject to public and regulatory scrutiny

Did you know that having a weather app on your phone could mean your personal movements are tracked second-by-second and sold to third parties, even when you're not using the app? That's the basis of a 2019 lawsuit filed by the Los Angeles City Attorney's office. The suit charges that the information on selling data to third parties was hidden in the privacy policy and privacy settings sections of the app, which "the vast majority of users" don't read.[2]

Many companies that collect location data claim it doesn't violate privacy because the data is anonymous, users consent to be tracked, and data is kept securely. But the *New York Times* investigation shows these claims don't always hold up to legal or regulatory scrutiny. For example, pings showing a daily route from a house to an office easily identify a person.

While phone apps supply much of the tracking data sold to third parties, cellular companies are also under fire. The four largest US cellphone carriers promised to stop selling location data in 2018, but two years later, the U.S. Federal Communications Commission (FCC) proposed hundreds of millions of dollars in fines because the carriers were found to continue selling customer data and violating agency rules to protect personal information.[3]

[2] Eriq Gardner, "All the Time and Money on California's New Privacy Law Wasted?" *The Hollywood Reporter*, 15 June 2020, www.hollywoodreporter.com.

[3] Drew FitzGerald and Sarah Krouse, "FCC Probe Finds Mobile Carriers Didn't Safeguard Customer Location Data," *The Wall Street Journal*, 27 February 2020, www.wsj.com.

COVID-19 raises the stakes for location tracking

The COVID-19 crisis led some governments to launch phone apps with geolocation tracking to trace an individual's contacts and to determine whether they are complying with quarantine and social-distancing directives. Tracking individuals has helped some countries limit the virus's spread, but a Guardsquare security analysis of 17 government tracking apps found the "vast majority" are easy for hackers to breach.[4]

Human rights groups are concerned these apps are too invasive and could be used beyond the pandemic. For example, Norway's Data Protection Authority banned its country's tracking app after determining it collected far more data than needed.[5]

Businesses are also exploring new technologies to protect the health of their employees, using smartphone apps, cameras or wearable Bluetooth devices to monitor employee movement at work. If an employee tests positive for COVID-19, the company can quickly identify employees who came close to the infected worker. While many countries allow employers to track employees during work hours, privacy advocates fear surveillance could be extended around the clock and continue long after the crisis ends.

The pandemic has also raised privacy concerns with employee health data. An IAPP-EY survey published in May 2020 found nearly a quarter of businesses have taken their employees' temperatures, and 60% keep records of those diagnosed with COVID-19. Nearly one in five provided the names of COVID-19-positive employees to other staff or government authorities, contrary to the advice from the European Data Protection Board.[6]

4 Grant Goodes, "The Proliferation of COVID-19 Contact Tracing Apps Exposes Significant Security Risks," 18 June 2020, www.Guardsquare.com.

5 Scott Ikeda, "After Being Ranked Among the World's Most Privacy-Invasive, Norway Suspends Use of Contact Tracing App," *CPO Magazine*, 2 July 2020, www.cpomagazine.com.

6 Müge Fazlioglu, "Privacy in the Wake of COVID-19: Remote Work, Employee Health Monitoring and Data Sharing," IAPP-EY report, May 2020, https://iapp.org/resources/article/iapp-ey-report-privacy-in-wake-of-covid19.

Privacy regulations aim to control location tracking

The rising interest in protecting privacy has led to new regulations around the world. One of the most influential statutes, the General Data Protection Regulation (GDPR) of the EU, treats location data as personal data. This means users must specifically and freely agree to location tracking, rather than opting out. Google's lead data regulator in Europe launched a new investigation in 2020 after complaints that Google manipulated users into providing their location data. Google says it's constantly working to improve user controls and transparency.[7]

Location tracking is also addressed by the California Consumer Privacy Act (CCPA), which the state began enforcing in July 2020. Under the CCPA, California residents can opt out of having their personal information, including geolocation data, sold to third parties. While the law covers only state residents, many large firms are extending its rights to all Americans. California's attorney general estimates businesses will spend more than US$55 billion to comply with the CCPA.[8]

If your company sells location data, consider adhering to these GDPR requirements:

- Ask in clear and simple terms for freely given, specific and informed consent for location data, rather than simply requiring users to opt out.
- Clearly inform customers what types of location data you will process, what it will be used for, how long you will keep it and whether it will be sold to third parties.
- Before engaging third parties, review their ability to secure data properly and meet GDPR requirements.

7 Natasha Lomas, "Google's location tracking finally under formal probe in Europe," *TechCrunch*, 4 February 2020, www.techcrunch.com.

8 "Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations," prepared for California Department of Justice Office of the Attorney General, August 2019, dof.ca.gov.

Addressing privacy risks from location tracking requires cross-functional collaboration

Addressing privacy risks related to location tracking goes beyond the scope of legal and compliance departments. It requires flexibility and agility as organizations respond to fast-evolving technological and regulatory environments. Cross-functional collaboration is essential as it impacts a wide range of stakeholders. Legal and compliance professionals should take the lead in working with other functions — particularly IT departments — to help them identify, monitor and mitigate risks. Businesses need to keep privacy concerns in the forefront as they develop products or services that involve location tracking features. Talent management should focus on employee education and communication so that when used, location tracking doesn't compromise employees' privacy and its objective is well understood by employees. Information security and technology professionals need to stay on top of the rapidly evolving technologies to understand their impact and potential risks. Above all, privacy by design should be woven into the organizational culture.

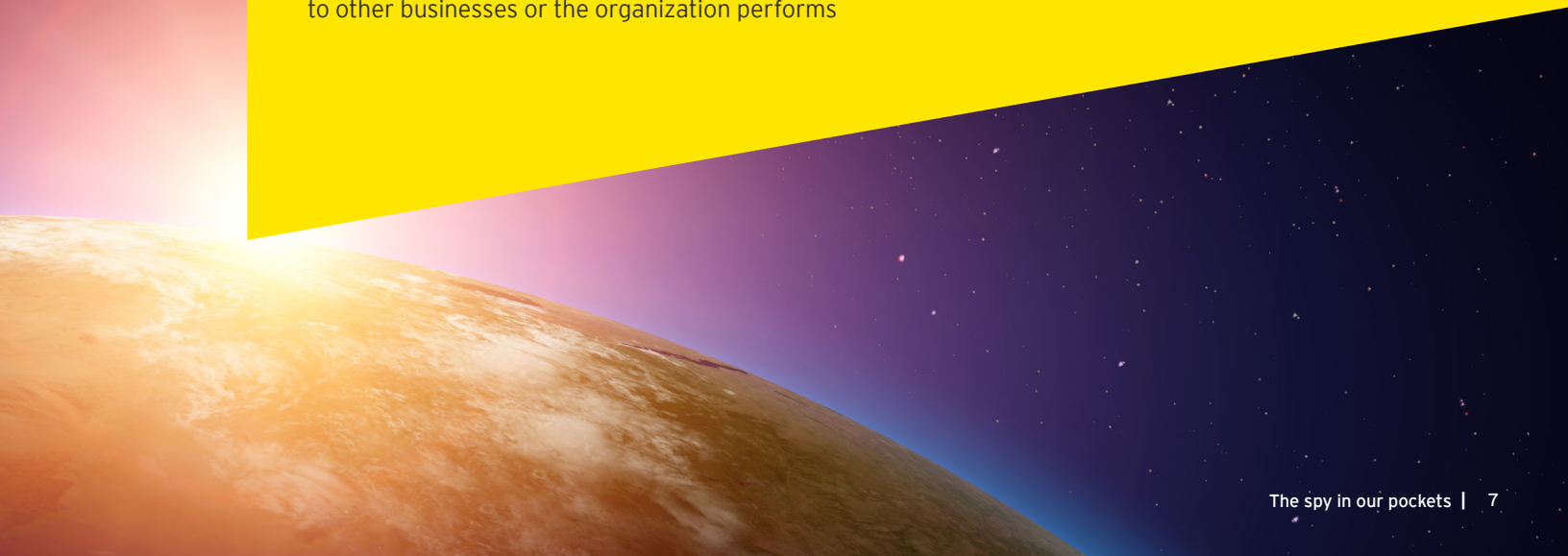
If not managed well, location tracking can become a huge liability that runs the risk of regulatory noncompliance, lawsuit, reputation damage, employee discontent and revenue loss. If managed well, location tracking can enhance product capability, boost service delivery and protect employees and the organization.

Key takeaways

Location tracking is becoming an important privacy concern, as it is increasingly used in many software applications that dominate our daily personal and business lives. The COVID-19 pandemic has heightened the issue as governments and organizations race to contain the spread of the virus. Businesses that hastily made operational changes during the pandemic, such as tracking employee movements or sharing personal health data, need to carefully evaluate their impact on privacy.

Compliance professionals should work collaboratively across the enterprise to mitigate risks around location tracking, whether the business markets data to other businesses or the organization performs location tracking on employees for internal purposes. These risks can result in regulatory and legal actions, data breach, employee morale and privacy concerns, as well as damage to the brand.

Adhering to data privacy regulations can be expensive and challenging. But businesses that manage location tracking activities transparently and securely will discover a competitive advantage as privacy protection becomes more important for both consumers and employees. We may love our phones but we don't want them spilling our secrets.



EY | Assurance | Tax | Strategy and Transactions | Consulting

About EY
EY is a global leader in assurance, tax, strategy, transaction and consulting services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. For more information about our organization, please visit ey.com.

About EY Forensic & Integrity Services
Embedding integrity into an organization's strategic vision and day-to-day operations is critical when managing complex issues of fraud, regulatory compliance, investigations and business disputes. Our international team of more than 4,000 forensic and technology professionals helps leaders balance business objectives and risks, build data-centric ethics and compliance programs, and ultimately develop a culture of integrity. We consider your distinct circumstances and needs to assemble the right multidisciplinary and culturally aligned team for you and your legal advisors. We strive to bring you the benefits of our leading technology, deep subject-matter knowledge and broad global sector experience.

EYG no. 005657-20Gbl
WR #2007-3544685
ED None

ey.com