MITRE | Intelligence After Next

2025 PRESIDENTIAL TRANSITION SPECIAL EDITION

SURVEILLANCE TECHNOLOGIES ARE IMBEDDED INTO THE FABRIC OF MODERN LIFE—THE INTELLIGENCE COMMUNITY MUST RESPOND

by Kirsten Hazelrig

As part of MITRE's support to the 2025 Presidential transition, we are highlighting key Intelligence After Next (IAN) papers published recently to stimulate thought, dialogue and action for intelligence and national security leaders. Key topic areas include surveillance, privacy, transparency, and accountability; foreign policy; counterterrorism and cybersecurity strategies; combatant command support; and the future of the IC workforce. IAN papers aligned to these topic areas address key policy, acquisition and warfighting concerns and are as relevant in 2025 as when first published.

Surveillance Technologies Present National Security Risk

As we interact with our phones, websites, and the digital ecosystem, ubiquitous surveillance generates vast amounts of commercial data that creates enduring records of our identity, locations, and connections. This commercial surveillance data is collected, repackaged, and sold in a vast and largely unregulated commercial market and is readily available for purchase by companies around the world and by our adversaries. Despite its omnipresent nature, many national policymakers still do not fully appreciate the overarching national security considerations of commercial surveillance technology that continuously collects personal information, ostensibly to better tune advertising. The intelligence potential of this Advertising Technology or "AdTech" data is immense, and America's adversaries are leveraging commercial AdTech data to enhance their asymmetric capabilities. To date, there is ample open-source evidence that these commercial capabilities can be used to:

- Target influential individuals for blackmail and coercion[1]
- Physically map and target sensitive sites, security measures, high risk personnel, and operations[2] [3]
- Create near real-time situational awareness of U.S. soft targets[4, 5]
- Target offensive cyber operations and network exploitation[6]

To address these threats, the U.S. must first consider what information is collected and then focus on ways to mitigate the greatest risks associated with the AdTech ecosystem. By understanding these risks and applying effective countermeasures such as regulation and industry collaboration, the U.S. can reduce their impacts. We have seen, for example, some reduction in data points available from countries under the General Data Protection Regulation, and immediately following Apple's App Tracking Transparency initiative.[7]

ADTECH—What is it?

AdTech is the collective term for the commercial ecosystem of tools, technologies, infrastructure, and organizations that track and monetize human behavior. The AdTech industry has experienced explosive growth in recent years. This growth, combined with rapidly changing regulation, maturing commercial policies, evolving technologies, and the sheer volume of data and money involved creates an extremely challenging environment. We do know, however, that the data generated by this ecosystem uniquely supports granular intelligence on the U.S. population at large. According to European researchers, just the real-time bidding platforms that deliver ads expose the online activity and location of an average person in the U.S. 747 times per day, 57% more often than Europeans, regardless of whether the user ever sees an ad.[8]

> Mobile devices can continuously record location data elements, even if the device has location services disabled, is powered off, or is without service.

How is This Data Collected?

As companies gather more and more information about consumers and their habits to sell targeted advertising, build customized services, and improve the customer experience, there are innumerable methods used to harvest data and convert it into a usable form. Some are highly focused, while others are universally used. Identified risks include:

- **Mobile Apps.** Users knowingly share or input all types of information in an app, all of which may be visible to the app developer, and which may be sold or shared with third parties. This can include health information, personality quizzes, dating preferences, and other highly personal insights. Examples of nonvisible data includes user and system preferences, log-in information, and images—often including location, contacts, photos, and other personal information. Most mobile devices will ask the user for permission before granting sensitive device permissions to an app, however, this practice is neither universal nor comprehensive. Privacy policies purport to list how an app gathers, stores, and uses the information it collects from users; however, these are frequently inaccurate or incomplete. In addition, modern software such as web browsers and mobile apps rely upon Software Development Kits (SDKs), Application Programming Interfaces (APIs), and other third-party code bases to function, meaning that even the app developer may not fully know how all elements function within their own app.
- **Software Development Kits (SDK)** are a set of tools and programs used by developers to create or augment applications, provide an interface for specific platforms, and generate revenue for their apps. Understanding the scope of SDK data collection is often difficult. An SDK may have access to not only all data in an app, but also additional permissions on a device. The average mobile application contains 18.2 SDKs, with developers incentivized to integrate additional data harvesting SDKs.[A] As many SDKs use encrypted communications, understanding data transmitted requires forensic analysis and control over the device in question, combined with a weakening of security protocols on that device. Once the data leaves the device, it becomes virtually untraceable as it is conveyed to any number of third parties.
- **Application Programming Interfaces (APIs)** allow software to interact with other software. APIs are used to allow interactions between different systems, request data from servers, or render data into a viewable format; however, gaps in API control enforcement can allow advertising partners extensive access to user data, beyond the intention of the platform. The 2018 Facebook Cambridge Analytica scandal featured a political consulting firm exploiting API access to harvest the data of 50 million users, using it to micro-target political messaging and information campaigns both on and off the social media platform.[9]
- **Browser-Based Collection.** Web browsers can collect and link vast amounts of device and user activity such as browsing history, usage data, and locations. This often goes far beyond what is necessary for web browsing. For example, although most apps must request permission to use most mobile device sensors, mobile browsers can generally collect motion, orientation, proximity, and light sensor data without user consent.
- **Device Fingerprinting** defines an approach to identify a user's device based on operating system, IP address, contacts, apps and other specific signatures. It allows users to be de-anonymized, identified and tracked.

A. In 2021, privacy watchers determined that the UK-based location services company Huq was paying app developers to include an SDK which did not honor the privacy settings of the device and, on some devices, was sharing the data regardless of user opt-in.

What Data is Involved?

An essential premise of monetizing harvested data is the ability to link it to devices and individuals. In the past five years, increased regulation and the widespread adoption of privacy-enhancing technologies began to shift industry away from traditional identifier technologies, such as device IDs and third-party cookies and toward identifying individual users and tracking them across platforms. As traditional identifiers lose favor, new identity-alternative approaches seek to fill the gaps. Commercially available services merge different data sets, making it trivial to deanonymize at the individual level.[10]

The data that circulates through the AdTech ecosystem can be segmented into four general types: location and environmental; behavioral; demographic and psychographic; and transactional. Mobile device data forms the bulk of AdTech, but what that contains is often unanticipated by the user. Mobile device sensors are a rich source of data—they collect information about the environment including sound, lighting, temperature, barometric pressure, geomagnetic fields, and elevation; movement of the device—angle held, rotation, acceleration, and other factors.[B] Analysis of detailed sensor data can give insights such as: how fast an individual is moving; if they are sitting or standing; or if they are in the proximity of weapons fire. Given the accuracy of sensor data, it alone can provide location information, even if the device's location tracking capabilities have been disabled. For example, readings from a device's elevation (altimeter) and movement (accelerometer), combined with basic geospatial analysis techniques, can provide accurate locational information.[C, 11]

Further analysis combining demographic data with additional collected information to understand motivations and desires of a particular group is known as psychographic segmentation. Combined, these create a descriptive profile of a person, such as: "likes going to bars with friends," or "young mother who enjoys the outdoors." These profiles can be used to customize advertising to influence on a personal and emotional level and can also be used to target groups without needing to identify individual targets.[12] As early as 2014, U.S. security researchers identified threat actors successfully exploiting defense industrial base networks by targeting malwarelinked ads to users with interest profiles, device attributes, and geolocation history that linked them to military targets.[D]

Adversarial Use

The AdTech environment offers significant intelligence potential, but also exposes organizations, individuals, and operations to significant risk as our adversaries are leveraging commercial AdTech data to provide asymmetric capabilities. The Intelligence Community (IC) should address these near-term concerns first:

- Constraining **Surveillance and Geolocation Tracking**. AdTech-enabled surveillance technologies are legitimately sold for law enforcement and counterterrorism uses; however, the industry has a pattern of vendors that sell products indiscriminately, operate proxy organizations to evade controls, and otherwise enable use of these powerful tools by adversaries that would not otherwise have such technologies, especially across the Middle East, Africa, and the developing world.

B. Although most apps must request permission to use most sensors, mobile browsers can generally collect motion, orientation, proximity, and light sensor data without user consent.

C. In 2021, it was reported that U.S. company Facebook was constantly harvesting accelerometer data of all iPhones with one of its apps installed, regardless of privacy or location tracking settings. Analysis was able to infer the location of a given individual based only upon matching a device's vibrations to those of other individuals in the area.

D. Security firm Invincea dubbed this campaign "Operation DeathClick," stating at the time that its defense industrial base customers were six times more likely to experience targeted malvertising than comparable private sector companies.

- Reducing the vulnerability of **targeted cyber-attacks**. Micro-targeted advertising enables the targeting of malware-linked sites based on a combination of characteristics even if the targeted individuals themselves are not known to the threat actor.
- Countering **Information Operations**. The ability to micro-target information through paid promotion and the exploitation of content algorithms creates the ability to build belief silos in which an individual is exposed to a curated "truth" about given topics, or presented with specific messaging unique to their occupation, location, or other factors.[13, 14]

The IC must understand what information is collected and then effectively respond to the greatest risks presented by the AdTech's ecosystem. As risks are understood, countermeasures such as law, regulation, and strategic partnerships must be established to strengthen our national defense and enhance our collective and individual security.

Time for a Comprehensive Response Strategy

The data that flows through AdTech is poorly understood and the risk exposure is complex, especially when considered comprehensively across the whole of government and civil society. To protect the American people from these threats, the U.S. government needs to understand potential adversarial weaponization and national security impact. The IC is uniquely positioned to both have exquisite insights into adversarial capabilities and threats, as well as a detailed understanding of how the advanced analysis of these data sets can yield actionable insights. The IC should take action to understand and enumerate where in the ecosystem is there more risk and where effective countermeasures could strengthen defense and enhance security.

Mitigating a set of technologies and business practices that is held solely in private industry requires a broad government response, including regulation, enforcement actions, and sanctions or other attempts to dissuade egregious actors once norms and regulations are in place.

References

1. Lati, M. and Boorstein, M. "Case of high-ranking cleric allegedly tracked on Grindr app poses Rorschach test for Catholics." The Washington Post, 21 July 2021. https://www.washingtonpost.com/religion/2021/07/21/catholic-official-grindr-reaction/
2. Hsu, Jeremy. "The Strava Heat Map and the End of Secrets." Wired.com, 29 Jan 2018. https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/
3. Thompson, S. and Warzel, C. "How to Track President Trump." The New York Times, 20 Dec 2019. https://www.nytimes.com/interactive/2019/12/20/opinion/location-data-national-security.html
4. Silverman, C. "Google allowed sanctioned Russian ad company to harvest user data for months" Ars Technica, 5 July 2022. https://arstechnica.com/information-technology/2022/07/google-allowed-sanctioned-russian-ad-company-to-harvest-user-data-formonths/
5. Thompson, S. and Warzel, C. "One Nation, Tracked." The New York Times, 19 Dec 2019. https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html
6. Patterson, D. "Campaign 2018: New malware attacks target voters in key battleground states," 26 Oct 2018. https://www.cnet.com/news/privacy/campaign-2018-new-malware-attacks-target-voters-in-key-battleground-states/
7. Kollnig, K. et al. "Goodbye Tracking? Impact of iOS App Tracking Transparency and Privacy Labels," 7 May 2022. https://arxiv.org/abs/2204.03556
8. Irish Council for Civil Liberties. "The Biggest Data Breach." 16 May 2022. https://www.iccl.ie/digital-data/iccl-report-on-the-scale-of-real-time-bidding-data-broadcasts-in-the-u-s-and-europe/
9. BBC.com "Cambridge Analytica parent firm SCL Elections fined over data refusal," 10 Jan 2019. https://www.bbc.co.uk/news/technology-46822439
10. Cox, J. "Inside the Industry That Unmasks People at Scale," Vice, 14 Jul 2021. https://www.vice.com/en/article/epnmvz/industry-unmasks-at-scale-maid-to-pii
11. Ikeda, S. "Cambridge Analytica parent firm SCL Elections fined over data refusal." CPO Magazine, 5 Nov 2021. https://www.cpomagazine.com/data-privacy/facebooks-use-of-alternate-location-tracking-methods-to-circumvent-apple-privacyprotections-expands-to-accelerometer-data/
12. Newman, L.H. "Facebook Ad Services Let Anyone Target U.S. Military Personnel," Wired.com,28 Jan 2021. https://www.wired.com/story/facebook-ad-targeting-us-military/
13. Issenberg, S. "Obama's White Whale." Slate Magazine, 15 Feb 2012. https://slate.com/news-and-politics/2012/02/project-narwhal-how-a-top-secret-obama-campaign-program-could-change-the-2012-race.html
14. Dawson, J. "Microtargeting as Information Warfare," The Cyber Defense Review, Winter 2021. https://cyberdefensereview.army.mil/Portals/6/Documents/2021_winter_cdr/04_CDR_V6N1_Dawson.pdf

Author

Kirsten Hazelrig is a former cyber policy lead at MITRE, focused on deception, digital surveillance, and influence operations. She began her career working with military and law enforcement to develop cyber intelligence capabilities and has continued to work to enable the understanding and countering of threat actor activity. She currently serves as a Mission Manager in the ODNI's Cyber Threat Intelligence Integration Center.

Intelligence After Next

MITRE strives to stimulate thought, dialogue, and action for national security leaders developing the plans, policy, and programs to guide the nation. This series of original papers is focused on the issues, policies, capabilities, and concerns of the Intelligence Community as it prepares for the future. Our intent is to share our unique insights and perspectives surrounding a significant national security concern, a persistent or emerging threat, or to detail the integrated solutions and enabling technologies needed to ensure the success of the Intelligence Community. The views expressed in this publication are those of the author(s) and do not imply endorsement by the Office of the Director of National Intelligence or any other U.S. government department/agency.

You can receive all of MITRE's Intelligence After Next papers by subscribing to the series at mitre.org/IntelligenceAfterNext

About MITRE

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded research and development centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

JANUARY 2023