Journal of Information Systems Education

Volume 37
Issue 3
Summer 2026

Teaching Case

No Place to Hide: Ethical and Legal Challenges in Geospatial Consumer Targeting

Christine Ladwig and Dana Schwieger

Recommended Citation: Ladwig, C., & Schwieger, D. (2026). Teaching Case: No Place to Hide: Ethical and Legal Challenges in Geospatial Consumer Targeting. *Journal of Information Systems Education*, 37(3), 397-412. https://doi.org/10.62273/KRTU5903

Article Link: https://jise.org/Volume37/n3/JISE2026v37n3pp397-412.html

Received: March 30, 2025
First Decision: June 29, 2025
Accepted: May 22, 2026
Published: September 15, 2026

ISSN: 2574-3872 (Online) 1055-3096 (Print)

Journal of Information Systems Education, 37(3), 397-412, Summer 2026
https://doi.org/10.62273/KRTU5903

Teaching Case
No Place to Hide: Ethical and Legal Challenges in Geospatial Consumer Targeting

Christine Ladwig
Dana Schwieger
Harrison College of Business and Computing
Southeast Missouri State University
Cape Girardeau, MO 63701, USA
cladwig@semo.edu, dschwieger@semo.edu

ABSTRACT

Advertising has evolved beyond traditional media to dynamic, artificial intelligence (AI) and data-driven displays that interact with passersby. Marketers now use various technologies to collect and combine geospatial and personal data from drivers and pedestrians, often without their explicit consent. The rise of geotargeted advertising and its use of geospatial imaging and geofencing has sparked debates over surveillance, data security, and the extent of consumer rights. As companies increasingly use these technologies to deliver targeted advertising to mobile devices penetrating their geofenced borders and beyond, these activities raise both legal and ethical privacy concerns; the practice of geotargeting has even been classified as an "unfair or deceptive practice" in some instances. This teaching case, which focuses on real-world legal scenarios of geotargeted advertising, is intended to facilitate critical thinking about the intersection of geospatial technologies and privacy rights. The case can be used to illustrate the strategic use of geospatial technologies in business and to initiate discussion across multiple IS2020/CC2020 competency areas, including privacy, ethics, professionalism, and data security.

Keywords: Teaching case, Geospatial data, Privacy, Targeted advertising, Ethics, Geofencing

1. CASE SUMMARY

This teaching case introduces students to the ethical and privacy concerns surrounding location-based data by describing two legal actions: *In the Matter of InMarket Media, LLC* (FTC, 2023) and *United States v. InMobi Pte Ltd.* (2016). The *InMarket Media* case centered on the tracking, collection, segmentation, and use of consumer data to deliver targeted advertising. InMarket Media used consumer device coordinates and feeds to identify when smartphones entered or exited specific locations—such as grocery stores, hospitals, or doctors' offices—by collecting location-related data (e.g., IP address, longitude, latitude). Data was compiled and segmented to describe various customer audiences, then sold to brands and advertising agencies for use in targeted advertising. Although InMarket Media neither admitted nor denied the allegations in the legal action, the FTC (Federal Trade Commission) ordered the company to make significant changes to its business processes (FTC, 2024).

In the case of mobile advertising company InMobi Pte Ltd., app developers were able to monetize their apps by integrating InMobi's software development kit (SDK). InMobi offered geo-targeting tools that tracked users' locations—even when users had disabled location permissions. Until December 2015, the

company inferred location data through nearby Wi-Fi networks and, in some cases, collected precise latitude and longitude coordinates to build its own geolocation database. It also served geo-targeted ads regardless of app developers' intentions or users' privacy settings. Despite marketing claims that location tracking required user opt-in consent, developers using the SDK unknowingly deployed apps that tracked users without permission, undermining their own privacy policies. InMobi also failed to implement effective safeguards under the Children's Online Privacy Protection Act (COPPA), resulting in the unlawful collection of personal data from children under 13. These cases highlight broader risks associated with geolocation and geofencing technologies, particularly how geotargeted advertising can expose sensitive personal data and create ethical and privacy concerns for both businesses and consumers.

2. CASE

"Neither privacy nor publicity is dead, but technology will continue to make a mess of both."
—Danah Boyd

2.1 One in a Million: *United States v. InMobi Pte Ltd.* (2016)

Imagine walking downtown in New York's Times Square. Surrounded by thousands of people, you would think you are fairly anonymous within the crowd. The reality, however, is that the digital billboards also present in Times Square are working overtime to collect data from your phone, identifying not only who you are, but where you have been both physically and virtually (Germain, 2019). The information being gathered about you at that moment may be used to target advertising in a very public way—like a projection on a smart billboard—or to provide an endless stream of unwanted personalized digital ads on smart devices.

This is the scenario at the heart of the case *United States v. InMobi Pte Ltd.* (2016), the settlement of which marked a significant moment in the intersection of advertiser geotracking and consumer privacy rights (Sterling, 2016). InMobi, with U.S. operations based in San Francisco County, California, was a mobile-first advertising development platform that allowed Android and iOS mobile app developers to "monetize their application[s] by allowing third party advertisers to advertise to consumers through various ad forms, such as banner ads, interstitial ads, and native ads" (*United States v. InMobi Pte Ltd*., 2016, p. 3). Advertisers could use any InMobi SDK-integrated mobile application to target consumers.

InMobi offered advertisers multiple geo-targeting products that could target consumers based upon their physical location. Until December 2015, InMobi still often tracked a phone's location even though the owner had restricted API location access. In addition, InMobi would send geo-targeted ads to consumers "regardless of the application developer's intent to include geo-targeted ads in the application and regardless of the consumer's location settings" (*United States v. InMobi Pte Ltd*., 2016, p. 6). On devices in which the location API was accessible, InMobi would collect the latitude/longitude coordinates of the device as well as Wi-Fi network information and use triangulation to correlate the two sets of information to "create its own geocoder database through which it [could] match specific WIFI networks to specific locations" (*United States v. InMobi Pte Ltd*., 2016, p. 6).

Marketing materials for InMobi geo-targeted ad products, however, indicated that they only tracked the consumer's location and served geo-targeted ads upon opt-in consent by consumers. Software developers who used the InMobi SDK unknowingly created products that tracked consumers regardless of their preferences, thereby undermining the privacy practices of their app customers. In addition, InMobi "neither implemented adequate privacy controls to ensure its compliance with COPPA [Children's Online Privacy Protection Act] nor tested that the controls that it had implemented functioned as intended" (*United States v. InMobi Pte Ltd*., 2016, p. 12). Thus, InMobi-supported devices collected and used the personal information of children under 13, violating COPPA.

2.2 When Privacy Follows You Home: *In the Matter of InMarket Media, LLC* (FTC, 2023)

Imagine stepping quietly into a local addiction recovery center, seeking nothing more than a moment of support and privacy. You never take your phone from your pocket. However, that evening, as you casually

open a weather app, the screen fills with ads—rehabilitation programs, counseling services, prescription treatment options—eerily specific, almost as if they were waiting for you. The same kinds of ads begin to trail you from app to app, quietly shadowing your digital life. You are left with a lingering, unsettling question: How did they know where you were—and why are they following you now?

This is the issue at the center of *In the Matter of InMarket Media, LLC* (FTC, 2023), where the technologies and processes used by InMarket included collecting copious amounts of personal data about users over time, including their purchasing history, demographic and socioeconomic backgrounds, as well as movement tracking of their mobile device. The data was categorized into specific audience groups and sold to InMarket Media's clients (brands and advertising agencies) for targeted advertising (FTC, 2023). "One of the primary functions of the InMarket SDK is to transmit a consumer's precise location back to Respondent" (FTC, 2024, p. 2). Apps that incorporated the InMarket SDK could transmit to InMarket a unique identifier for the mobile device, its precise latitude and longitude, and a timestamp as often as the mobile device's operating system allowed, ranging from zero data transmissions when the device was idle up to data transmissions every few seconds when the device was in motion. From 2016 until the filing of the complaint, "about 100 million unique devices sent Respondent location data each year" (FTC, 2023). The InMarket SDK enabled the collection of sensitive information about consumers' daily movements, such as where individuals lived, worked, worshipped, took their children to school or childcare, and received medical care (possibly even revealing a medical condition) (FTC, 2023, p. 2). The InMarket SDK displayed focused ads in specified apps and offered advertisers a product that would send targeted push notifications to consumers passing through geofenced areas.

The case concluded with a consent agreement in which InMarket did not admit nor deny the allegations in the complaint. The FTC's order required InMarket to change its business practices, including prohibiting the material misrepresentation of the collection and use of location data, the sale or licensing of location data, and the categorization of data for targeting consumers based on location data identified as sensitive. In addition, InMarket was required to develop a formal Sensitive Location Data Program, only collect data when affirmative express consent had been obtained, provide consumers with easy opt-out and deletion mechanisms, adhere to data-retention limits, develop an SDK supplier assessment program, and notify prior consumers of the data collection and delete or deidentify all historical data (FTC, 2024).

3. BACKGROUND INFORMATION: GEOTARGETING AND ADVERTISING

3.1 Geospatial Technology Use in Marketing

The integration of geospatial data collection into advertising, as seen in the InMobi and InMarket cases, has transformed traditional consumer-targeting methods. The use of data collection technologies, such as Bluetooth beacons, Wi-Fi sniffers, cameras, location-based apps, and other devices, by digital marketers is contributing to growing privacy concerns (Lewinski et al., 2016). Geofencing, geotracking, and geotargeting are enabling advertisers to deliver highly personalized advertisements and communications based on an individual's location and behavioral patterns (Germain, 2019).

Geofencing technologies create a virtual boundary around a geographic area that triggers an action when a smart device enters or leaves the area (Holt, n.d.; Maximum Media & PR, 2024; Shevchenko & Reips, 2023; UMATechnology, 2024). Geotracking devices are more invasive, as they continuously track a device's absolute geographic location via periodic position notifications (Melekhova et al., 2010). The use of geotargeting in advertising allows marketers to send marketing materials not only to consumers at the appropriate location but also at the appropriate time. Thus, analysis of the target's time-use-activity patterns would be required (Banerjee et al., 2013).

While these innovations may enhance marketing efficiency, they also raise concerns about personal privacy (McKenzie et al., 2019) and informed consent. For example, research has shown that even anonymized location data can often be re-identified, exposing individuals to risks such as surveillance and unwanted data sharing (Holder, 2019). A study from MIT and the Université Catholique de Louvain analyzed 15 months of supposedly anonymized mobile phone data from approximately 1.5 million European users. Despite the anonymization, they discovered that just four spatiotemporal points—locations

at specific times—were sufficient to identify 95% of individuals in the dataset uniquely. Even more alarming, approximately half of the users could be re-identified using only two data points. According to the researchers, "little outside information is needed to re-identify the trace of a targeted individual even in a sparse, large-scale, and coarse mobility dataset" (Jones, 2013).

3.2. Forms of Advertising Geotargeting: Geofencing

In general, most U.S. adults who carry smart devices are vulnerable to receiving geotargeted advertising through geofencing (Laningham, 2022). In a 2022 Harris Poll study of 1,054 U.S. adults, the survey found that "79% of U.S. adults report that they have location sharing features activated on the devices that they use some of the time" (Laningham, 2022, p. 1). Only 10% of the respondents reported never having location-sharing features enabled. Thus, many smart devices are vulnerable to marketers who are integrating geofencing with billboards and mobile devices to provide more targeted advertising by

- **Synchronizing and retargeting ads on mobile devices** with the visual content as the customers move through, and exit, the geofenced area;
- **Adjusting content in real time based** upon data collected through geofencing; and
- **Analyzing location and response data** collected in association with the geofenced area to optimize and improve audience engagement rates. Such engagement analytics include metrics such as foot traffic, mobile activity, in-store revenue, and brand awareness (Maximum Media & PR, 2024).

Personalized information obtained through location-based settings enables marketers to deliver more targeted advertising, as seen in the InMobi and InMarket cases.

3.3. Forms of Advertising Geotargeting: Smart Billboards

Although most geotargeted communications are directed toward specific devices, smart billboards are another advertising medium that serves as an intelligent platform powered by AI, sensors, cameras, and real-time data to deliver "the right message at the right time" (Nadeem, 2025, p. 1). These digital signs, placed in public or quasi-public spaces, can gather analytics of passersby such as foot/vehicle traffic density and patterns, facial expressions and demographics (age, gender), gestures, and behavior (e.g., time spent looking at a smart billboard), to display directed advertisements (Davis, 2020; Nadeem, 2025; New Target, 2024). For instance, in a crashed advertising app for a pizza shop in Oslo, the app described the person in front of the camera, providing details such as "young male, wearing glasses, where he was looking, whether he was smiling, and how much he was smiling" (Vaas, 2017, p. 1).

Companies are increasingly aligning geofencing and geospatial imaging with their advertising efforts (Germain, 2019). For example, the Paris-based company Quividi (established in 2006) was an early developer of small digital billboards equipped with tiny cameras to gather information about passersby, including the person's approximate age, gender, and the time they viewed the billboard. This information was transferred to a private central database, which could then tailor a digital display to the person standing in front of the billboard (CNET, 2008). Although Quividi claimed that photographs of the billboard visitors were not stored and that it detected all vehicles, bodies, and faces passing in front of the company's screens with over 90% accuracy, the activity raises privacy concerns. However, the fact that data gathered by smart billboards, such as Quividi, is not stored, or is stored in a way that makes "future identification impossible," makes the application of data protection rules difficult (Davis, 2020).

In 2015, Yahoo! applied for a smart billboard patent that collected data through sensors, cameras, and microphones (Ferguson, 2017). Yahoo!'s billboard would collect biometric data, as well as mobile device data and images, to "identify specific individuals in the target audience" and "identify specific vehicles and/or drivers" (Ferguson, 2017, p. 1). The billboard microphones enabled Yahoo! to record conversations to gauge the audience's reactions to ads. Built-in eye-tracking sensors could be used to determine whether and for how long a passerby viewed an advertisement. These tools, combined with the mobile data, allowed the advertiser to "form a more focused profile of the audience" (Ferguson, 2017, p. 1).

According to Jane Frost of the Market Research Society, the collection and use of geolocation data are evolving rapidly. However, data privacy legislation is not keeping pace (as cited in Henley, 2013). The

legal framework governing the use of these technologies remains ambiguous, potentially leaving human subjects vulnerable to exploitation (Newcomb, 2016).

3.4 Forms of Advertising Geotargeting: Mobile Device Location Tracking

Many individual mobile apps have location-tracking settings and features that users may be prompted to activate upon installation. Google, for instance, has Location Reporting and Location History, which are toggle settings on each device connected to a Google account, used to track users' movements. By default, each setting is turned off. However, once a user launches a location-based app, such as Google Maps, the toggle is switched on (Dobie, 2014). Once enabled, Google Location Reporting will periodically send its location to Google. Google Location History allows Google to store a record of all user location data from every device once enabled.

Google Chrome also has a Web & App Activity setting that saves users' activity on Google sites and apps, as well as a device's general location and IP address (Google, 2025). This setting is used to personalize Google ads and Google search content. Adjusting these settings can also provide a level of privacy protection for device users. These settings, however, can be accidentally modified when future apps open and request changes to improve performance. Many business-specific apps ask users to track their location. Thus, if a device enters a geofenced area that supports an app on its phone—as in the InMobi and InMarket cases—it may receive targeted communications associated with that app.

Marketers are additionally using geofencing technologies in "geo-conquesting" strategies to lure customers away from competitors on their home turf. For instance, in Hyundai's aggressive marketing campaign entitled "Dealer Stealer," Hyundai placed geofences around Mazda and Toyota dealerships in Australia and sent mobile ads to individuals located on their premises. Whole Foods Market placed geofences around competitor supermarkets and offered steep discounts to mobile device owners in those stores to encourage them to shop at Whole Foods. Dunkin Donuts created geofences around competitor coffee shops and sent discount coupons to their prospective customers (Chandra, 2021). Burger King enacted a similar strategy with its "Whopper Detour" campaign targeting McDonald's locations (EOM, n.d.). Such strategies are not illegal, but questions may arise about the ethical implications.

4. BACKGROUND INFORMATION: LEGAL CONSIDERATIONS

4.1 Geospatial Data Use Privacy Laws

Currently, there is no single national law in the United States that protects data privacy, let alone geospatial data privacy. However, as of July 2025, 38 states have passed privacy legislation or are in the process of reviewing it (Botero, 2026). There are also several federal acts that address different types of data, such as the Health Insurance Portability and Accountability Act (HIPAA), Fair Credit Reporting Act (FCRA), Family Educational Rights and Privacy Act (FERPA), Gramm-Leach-Bliley Act (GLBA), Electronic Communication Privacy Act (ECPA), Children's Online Privacy Protection Act (COPPA), and the Video Privacy Protection Act (VPPA) (Klosowski, 2021).

State legislatures are beginning to address geospatial data. For instance, Connecticut, Washington, Nevada, and New York are enacting legislative measures prohibiting geofencing advertising and data collection near health care facilities (Ehrhardt & Izzo, 2024). Under New York's General Business Law section 394-g, which took effect July 2, 2023, their standalone geofencing-focused law indicates that "it is unlawful in New York for any person or entity to set up a geofence around any health care facility except their own" (Ehrhardt & Izzo, 2024, p. 8). The law defines geofencing as the use of any technology to create a "virtual boundary of 1,850 [about 1/3 of a mile] feet radius, or less or 'geofence' around a particular location" and is used by digital advertisers to track the location of a mobile device to deliver targeted digital advertisements upon entry into the geofenced area (Ernhardt & Izzo, 2024, p. 8). In addition, the law implies that consumer health information cannot be obtained from a health care facility, including information about the patient's presence at a particular facility. "The law does not prohibit health care providers from establishing a geofence around their own facility" for the purpose of checking patients in and surveying

them regarding their facility experience as long as they abide by HIPAA and other relevant privacy and security legislation (Ehrhardt & Izzo, 2024, p. 9).

4.2 Privacy and Geospatial Data Use in Government

Widespread use of geotargeting technologies is now firmly established globally (Polaris Market Research, n.d.), but advertisers are not the only groups applying geofencing and geolocation surveillance to achieve their objectives.

For example, in 2022, the French government used geolocation (Google Earth) to identify undeclared swimming pools at regional residences. Land with a swimming pool is subject to higher property tax rates: An average pool of 30 square meters is taxed at €200 per year. Using artificial intelligence and advanced geolocation techniques, French authorities identified over 20,000 rogue swimming pools at a tax value of €10 million (Thompson, 2023).

A more controversial governmental use of geolocation surveillance is that employed by U.S. Immigration and Customs Enforcement (ICE). ICE relies on a range of location-based technologies and data sources to identify, track, and apprehend individuals suspected of immigration violations (Wang et al., 2022, p. 2). This includes mobile phone location data purchased from private data brokers, automated license plate reader (LPR) databases, cell tower records, and geofencing-style analytics (Wang et al., 2022, p. 7). Individuals are often unaware their location data is being collected and sold, and critics argue that government purchase of such data may bypass warrant requirements and infringe on Fourth Amendment protections (Wang et al., 2022, p. 33). There are also concerns about tracking people at sensitive locations such as medical facilities, places of worship, or legal offices, which could discourage individuals from seeking services or participating in civic life (Wang et al., 2022, p. 5). While these technologies may increase enforcement efficiency, they raise significant privacy and legal concerns.

Conversely, other governmental authorities are using geolocation to drive positive change for their citizens. Nigeria, for instance, uses geospatial analysis to help map maternal and child mortality risks and improve healthcare access (Henley, 2013). Authorities in the country, however, recognize that such data gathering and identification present risks. While geotargeting technologies may be used for a variety of societal and commercial purposes, the legal framework governing their use remains ambiguous, potentially leaving human subjects vulnerable to exploitation (Newcomb, 2016).

5. BACKGROUND INFORMATION: ETHICAL CONSIDERATIONS

Although legislative guardrails are fragmented and few, ethical frameworks are available that future computing professionals can use to supplement current legislative policies and offer further insights into ethical and privacy considerations.

5.1 Twenty-Nine Questions for Geospatial Data Use

The right to privacy is an important consideration in this increasingly technological global landscape. While digital advertising values the specificity afforded by smart billboards, geofencing, geo-conquesting, and other forms of "surveillance," these developments carry a distinctly negative connotation with the public. Advancements such as facial recognition software and real-time analytics are adding to the ethical conundrum, creating a challenging decision-making environment for businesses (Power et al., 2021).

How should these sophisticated new technologies, increasingly enhanced by AI, be evaluated ethically? Data professionals are not trained as ethicists or attorneys, and yet they are asked to make ethical decisions about their use (Power et al., 2021). Compliance with the law, of course, is paramount in any decision, but determining the most ethical option may be difficult.

In 1994, sociologist Gari T. Marx noted that principles of fair information practice adopted in the 1970s and updated throughout the 1980s to regulate the use of technology were woefully inadequate for modern personal surveillance and information technologies (Marx, 1994). He suggested 29 questions (see Appendix A) to help individuals and organizations determine the ethics of surveillance techniques (Marx, 1998, p. 2). The questions examine the surveillance method—whether it is targeted communication, a smart

billboard, geofencing, or facial recognition profiling—and the idea that the right to employ these technologies is accompanied by a duty to use them responsibly. Although written in 1998, Marx's questions still apply today.

5.2 Guidance From the ACM Code of Ethics

The software developer can also find guidance on the use of geospatial data in the Association for Computing Machinery (ACM) Code of Ethics (an excerpt from the Code is in Appendix B). Expressed in the ACM Code is "the conscience of the [computer science] profession" where "the public good is always the primary consideration" (ACM, 2018, p. 1). The Code emphasizes the need to "minimize negative consequences" on stakeholders, including "threats to health, safety, personal security, and privacy" (ACM, 2018, Section 1.1). Section 1.6 (Respect privacy) states that "technology enables the collection, monitoring, and exchange of personal information quickly, inexpensively, and often without the knowledge of the people affected." The passage encourages professionals to become familiar with the "…various definitions and forms of privacy," and notes that the professionals "should understand the rights and responsibilities associated with the collection and use of personal information" (ACM, 2018, Section 1.6). This aligns well with geospatial data and surveillance technologies.

5.3 Guidance From Privacy Directives

Privacy regulations and violation costs vary by region (McKenzie et. al., 2019). Two of the most well-known privacy directives are the European Union's General Data Protection Regulation (GDPR) and the United States' California Consumer Privacy Act (CCPA). GDPR encourages Privacy by Design, the practice of incorporating data protection measures into software from the initial design phase of development (European Parliament and Council of the European Union, 2016). Privacy by Design advocates "minimizing the processing of personal data, pseudonymizing personal data as soon as possible, transparency about the functions and processing of personal data, enabling the data subject to monitor the data processing, [and] enabling the controller to create and improve security features" (European Parliament and Council of the European Union, 2016, Article 78).

The CCPA advocates adopting similar development practices. Programmers are expected to adopt secure coding practices (ensuring that the code is not subject to exploits and ensuring the confidentiality of users), regularly updating and patching software, and employing technologies like secure access controls and firewalls" (HackerOne Team, 2024, p. 1). In addition, under CCPA, programmers must document their processes, including data processing activities, the data collected and its purpose, and measures taken to protect the data. By adopting "version control, automated testing, and integrating privacy" into the software development process, programmers can "ensure compliance and facilitate audits" (HackerOne Team, 2024, p. 1).

In line with current legislative requirements, the nonprofit foundation, the Open Worldwide Application Security Project (OWASP), published its Developer Guide in 2023 as a reference for application and system developers. OWASP is dedicated to improving software security through the provision of resources to enable "organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted" (OWASP, 2023, p. 5). The guide "describes security practices using the advice given in the OWASP Software Assurance Maturity Model (SAMM)" and serves "as a cross-reference source to the many tools and documents that OWASP provides for developers" (OWASP, 2023, p. 5).

Another resource for future developers is the National Institute of Standards and Technology (NIST), which provides a range of security frameworks and guidelines to reference when developing more secure systems. While legislative guardrails are still evolving, current legislation, codes of ethics, and programmer guides can be used by software developers to design privacy, ethical, and security-focused measures into AI and data-driven systems supported by personal and location-based data in the delivery of customized messages to groups and individuals.

6. PREPARING FOR THE FUTURE

As artificial intelligence (AI) and Internet of Things (IoT) technologies continue to be embedded into an increasing number of products and processes, ethical and privacy practices should become ever more important. Future computing professionals need to bear in mind the ethical issues that may arise and consider practicing ethics- and privacy-by-design philosophies in their development processes. This section provides opportunities to think through geospatial development scenarios using an ethical mindset through discussion questions associated with the previously described court cases, application of the ethical frameworks, and the evaluation of business scenarios.

6.1 Case Questions: One in a Million: *United States v. InMobi Pte Ltd.* (2016)

The following questions relate to the case described in Section 2.1.

1. If a user disables location services on their device, do companies like InMobi have any ethical justification for collecting location data through alternative means (such as Wi-Fi triangulation)?
2. Should app developers bear responsibility for privacy issues embedded in third-party SDKs (like InMobi's)?
3. Is a company ethically responsible for the incidental gathering of data about children who are not the target of their app?
4. Does the ability to collect detailed geolocation data create a duty of care for companies handling that data?
5. From a utilitarian perspective, do the benefits of targeted advertising outweigh the privacy risks in this case?

6.2 Case Questions: When Privacy Follows You Home: *In the Matter of InMarket Media, LLC (FTC, 2023)*

The following questions relate to the case described in Section 2.2.

1. Should visiting a sensitive location—such as a medical clinic, counseling center, or addiction recovery facility—be treated as private information?
2. Even if geofencing is legal, what, if any, ethical lines might a company cross when using location-based advertising?
3. Should laws like consumer protection statutes be expanded to specifically regulate geofencing and location-based profiling?
4. If you designed ethical guidelines for a company using geofencing, what safeguards would you require before allowing this type of advertising?

6.3 Applying Marx's 29 Questions

To examine the ethics of surveillance methods—whether targeted communication, smart billboards, geofencing, or facial recognition profiling—sociologist Gari T. Marx suggested 29 Questions (see Appendix A).

1. In the case *United States v. InMobi Pte Ltd.* (2016), advertisers used InMobi's SDK and deployed apps that identified users' locations and information.
    a) Apply Marx's 29 Questions to the development and sale of geotargeting tools that track users' data.
    b) Based upon what you learned from applying the 29 Questions, do you think the practice is ethical or unethical? Explain.
2. In the InMarket Media legal action, the software could use geofencing to identify when smartphones entered or exited specific locations—such as grocery stores, hospitals, or doctors' offices—by collecting location-related data.
    a) Apply Marx's 29 Questions to the use of geotargeting tools by advertisers to gather location data and employ that data to target consumers.

b) Based upon what you learned from applying the 29 Questions, do you think the practice is ethical or unethical? Explain.

6.4 Applying the ACM Code of Ethics

Section 1.2 (Avoid harm) of the ACM Code of Ethics states that computing professionals should, in their assigned duties, "ensure that all harm is minimized" (ACM, 2018, p. 4). How could you minimize the harm to others in the following circumstances related to the InMobi and InMarket cases?

1. In geospatial data collection and geofencing, consumers are often not fully aware that their data is being collected and used for advertising purposes.
2. Geofencing and other geotargeting practices collect large volumes of data, including location history and behavioral patterns.
3. The integration of facial recognition and AI-driven personalization, especially in smart billboards, has increased the ability to monitor public spaces.
4. Geofencing allows advertisers to target specific locations and demographics.
5. Currently, regulations on geofencing and other geotargeting practices vary by jurisdiction and lack a universal standard.

6.5 Case-Related Scenarios

The following scenarios describe the use of geospatial technologies in two different business situations to enhance the personalization of customers' experiences.

6.5.1 Hello Mini Driver. Butler, Shine, Stern and Partners (BSSP) created a personalized advertising campaign in which BMW Mini Cooper owners could volunteer to carry a key fob with an embedded RFID tag. When the fob was in the vicinity of a specified billboard, a personalized message written by the customer would display on the billboard, such as "Hi Neil, cool convertible" (Koeck & Warnaby, 2014, p. 1415).

1. If the company did not seek volunteers and used customer data collected during the vehicle purchase transaction, would the advertisement be legal? Why or why not?
2. Even if the unauthorized use of data was legal, is it ethical? Why or why not?
3. What potential harms could result from billboards displaying personalized messages to passersby?

6.5.2 Spotted & Served. An Oslo pizza shop ran personalized advertisements on a screen in their front window. The messages would change based upon the characteristics of the person standing in front of the connected hidden camera; for instance, meat-oriented ads were displayed to men and salad-oriented options to women. One day in 2017, the app powering digital content crashed, exposing its hidden facial recognition system. A passerby noticed the content of the crashed app's action log, which described him as "a young male, wearing glasses, where he was looking, whether he was smiling, and how much he was smiling" (Vaas, 2017).

1. What, if any, existing laws in your own area (e.g., data protection or location-tracking regulations) might this practice violate?
2. Even if this practice is legal in some areas, is it ethical? Why or why not?
3. Does use of the software abide by the ACM's Code of Ethics Preamble and Section 1.6 (Respect privacy)? Why or why not?

7. REFERENCES

Association for Computing Machinery (ACM). (2018). *ACM Code of Ethics and Professional Conduct.* ACM.org. https://www.acm.org/binaries/content/assets/about/acm-code-of-ethics-and-professional-conduct.pdf

Banerjee, S., Viswanathan, V., Raman, K., & Ying, H. (2013). Assessing Prime-Time for Geotargeting With Mobile Big Data. *Journal of Marketing Analytics*, 1, 174-183. https://doi.org/10.1057/jma.2013.16

Botero, D. (2026). *US State Privacy Legislation Tracker*. https://iapp.org/resources/article/us-state-privacy-legislation-tracker/

Chandra, A. (2021). Mobile Acquisition on Location: 3 Brands Using Geo-Conquesting to Win New Customers. *ANA Driving Growth.* https://www.ana.net/blogs/show/id/mm-blog-2021-02-using-geo-conquesting-to-win-customers

CNET. (2008). Billboards That Look Back. CNET. https://www.cnet.com/tech/tech-industry/billboards-that-look-back/

Davis, P. A. E. (2020). *Facial Detection and Smart Billboards: Analysing the "Identified' Criterion of Personal Data in the GDPR* (University of Oslo Faculty of Law Research Paper No. 2020-01). http://dx.doi.org/10.2139/ssrn.3523109

Dobie, A. (2014). *Understanding Google's Android Location Tracking*. Androidcentral. https://www.androidcentral.com/understanding-googles-android-location-tracking

Effortless Outdoor Media (EOM). (n.d.). *Strong Geofencing and Billboards: Targeting Audiences in Real-Time.* Effortless Outdoor Media. https://effortlessoutdoormedia.com/strong-geofencing-and-billboards/

Ehrhardt, J., & Izzo, F. (2024). New York Joins List of States Prohibiting Geofencing Near Health Care Facilities. *US Law Magazine*, 3, 8-9. https://www.rivkinradler.com/wp-content/uploads/2024/03/Geofencing-Near-Health-Care-Facilities_Rivkin-Radler.pdf

European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons With Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (Text With EEA Relevance). *Official Journal of the European Union.* https://eur-lex.europa.eu/eli/reg/2016/679/oj

Federal Trade Commission (FTC). (2023). *In the Matter of InMarket Media, LLC* (FTC File No. 202-3088). https://www.ftc.gov/legal-library/browse/cases-proceedings/2023088-inmarket-media-llc

Federal Trade Commission (FTC). (2024). *Decision and Order: In the Matter of InMarket Media, LLC* (FTC File No. 202-3088). https://www.ftc.gov/legal-library/browse/cases-proceedings/2023088-inmarket-media-llc

Ferguson, K. (2017). The Latest Trend in Data Collection — Smart Billboards That Look Back at You. *Humans of Data*. https://humansofdata.atlan.com/2017/02/data-collection-trend-smart-billboards/

Germain, T. (2019, November 20). Digital Billboards Are Tracking You. And They Really, Really Want You to See Their Ads. *Consumer Reports*. https://www.consumerreports.org/electronics-computers/privacy/digital-billboards-are-tracking-you-and-they-want-you-to-see-their-ads-a1117246807/

Google. (2025). Activity Controls. https://myactivity.google.com/activitycontrols

HackerOne Team. (2024). Data Privacy Regulations and Software Development: Navigating GDPR, CCPA, and Beyond. HackerOne. https://www.hackerone.com/blog/data-privacy-regulations-and-software-development-navigating-gdpr-ccpa-and-beyond

Henley, J. (2013, April 7). How Geolocation Technology Is Helping Save Lives in the Developing World. *The Guardian.* https://www.theguardian.com/technology/shortcuts/2013/apr/07/geolocation-technology-save-lives-developing-world

Holder, S. (2019). Car-Mounted Ads Take a New Direction: Data Collection. *Solutions Journalism Network.* https://storytracker.solutionsjournalism.org/stories/car-mounted-ads-take-a-new-direction-data-collection

Holt, R. (n.d.). Geofencing and Smart Billboards: Transforming Outdoor Advertising. *Blogtrepreneur.* https://www.blogtrepreneur.com/geofencing-and-smart-billboards-transforming-outdoor-advertising/

Jones, W. (2013). This Week in Cybercrime: "Anonymized" Cellphone Tracking Data Is Pure Fiction. *IEEE Spectrum.* https://spectrum.ieee.org/this-week-in-cybercrime-anonymized-cellphone-tracking-data-is-pure-fiction

Klosowski, T. (2021). The State of Consumer Data Privacy Laws in the US (And Why It Matters). *Wirecutter*. https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/

Koeck, R., & Warnaby, G. (2014). Outdoor Advertising in Urban Context: Spatiality, Temporality and Individuality. *Journal of Marketing Management*, 30(13-14), 1402-1422. https://doi.org/10.1080/0267257X.2014.909869

Laningham, A. (2022). Are Location Sharing Features More Than a Convenient Tool? *The Harris Poll.* https://theharrispoll.com/briefs/location-sharing-features/

Lewinski, P., Trzaskowski, J., & Luzak, J. (2016). Face and Emotion Recognition on Commercial Property Under EU Data Protection Law. *Psychology & Marketing*. 33(9), 729-746. https://doi.org/10.1002/mar.20913

Marx, G. T. (1994). New Telecommunication Technologies Require New Manners. *Telecommunications Policy,* 18(7). 538-551. https://doi.org/10.1016/0308-5961(94)90064-7

Marx, G. T. (1998). Ethics for the New Surveillance. *The Information Society*, 14(3), 171-185. https://doi.org/10.1080/019722498128809

Maximum Media & PR. (2024). How to Use Geo-Fencing With Billboard Advertising: A Practical Guide. https://www.maximummedia.ca/post/how-to-use-geo-fencing-with-billboard-advertising-a-practical-guide

McKenzie, G., Keßler, C., & Andris, C. (2019). Geospatial Privacy and Security. *Journal of Spatial Information Science,* 19, 53-55. https://doi.org/10.5311/JOSIS.2019.19.608

Melekhova, O., Abchir, M.-A., Châtel, P., Malenfant, J., Truck, I., & Pappa, A. (2010). Self-Adaptation in Geotracking Applications: Challenges, Opportunities and Models. In ADAPTIVE 2010: *2nd International Conference on Adaptive and Self-Adaptive Systems and Applications (ADAPTIVE 2010)*, 68-77. https://www.researchgate.net/publication/228461890_Self-Adaptation_in_Geotracking_Applications_Challenges_Opportunities_and_Models

Nadeem, R. (2025). How AI, Sensors & Real-Time Data Are Turning Billboards Into Smart Ads in 2025. *MediaFinch*. https://mediafinch.net/how-ai-sensors-and-real-time-data-are-turning-billboards-into-smart-ads-in-2025/

New Target. (2024). *Digital Billboard Advertising: Maximizing Impact in a Mobile-First World.* https://www.newtarget.com/web-insights-blog/digital-billboard-advertising/

Newcomb, D. (2016). New Digital Billboards Can Watch Your Speed, Scan Your Car at Traffic Lights. *Forbes*. https://www.forbes.com/sites/dougnewcomb/2016/08/14/new-digital-billboards-can-watch-your-speed-scan-your-car-at-traffic-lights/

Open Worldwide Application Security Project (OWASP). (2023). *OWASP Developer Guide.* https://owasp.org/www-project-developer-guide/release/introduction/

Polaris Market Research. (n.d.). *Location Based Advertising Market Size Worth $386.77 Billion by 2032.* https://www.polarismarketresearch.com/press-releases/location-based-advertising-market

Power, D. J., Heavin, C., & O'Connor, Y. (2021). Balancing Privacy Rights and Surveillance Analytics: A Decision Process Guide. *Journal of Business Analytics*, 4(2), 155-170. https://doi.org/10.1080/2573234X.2021.1920856

Shevchenko, Y., & Reips, U.-D. (2023). Geofencing in Location-Based Behavioral Research: Methodology, Challenges, and Implementation. *Behavior Research Methods*, 56, 6411-6439. https://doi.org/10.3758/s13428-023-02213-2

Sterling, G. (2016). InMobi to Pay Nearly $1 Million Following FTC Charges of Location Tracking Deception. *MarTech*. https://martech.org/inmobi-pay-nearly-1-million-following-ftc-charges-location-tracking-deception/

Thompson, H. (2023). Tax Authorities Discover 120,000 Undeclared Swimming Pools in France. *The Connexion.* https://www.connexionfrance.com/practical/tax-authorities-discover-120000-undeclared-swimming-pools-in-france/107218

UMATechnology. (2024). What Is "Geofencing"? UMA Technology.com https://umatechnology.org/what-is-geofencing/

United States v. InMobi Pte Ltd. (2016). https://www.ftc.gov/system/files/documents/cases/160622inmobicmpt.pdf

Vaas, L. (2017). Would You Like a Side of Facial Recognition With Your Pizza? *Sophos News.* https://news.sophos.com/en-us/2017/05/11/would-you-like-a-side-of-facial-recognition-with-your-pizza/

Wang, N., McDonald, A., Bateyko, D., & Tucker, E. (2022). *American Dragnet: Data-Driven Deportation in the 21st Century*. Center on Privacy & Technology at Georgetown Law. https://americandragnet.org/sites/default/files/American_Dragnet_report_English_final.pdf

AUTHOR BIOGRAPHIES

Christine Ladwig is a Professor of Business Law in the Harrison College of Business and Computing at Southeast Missouri State University. Dr. Ladwig holds a JD-M.Acc. joint degree from Southern Illinois University–Carbondale, an LL.M. in Intellectual Property Law from Albany Law School (Union University), and a Ph.D. in Biology from The George Washington University. Her research interests include information systems liability, intellectual property and business valuation, and business law and ethics. She has published in *Information Systems Education Journal*, *Journal of Case Studies*, *Journal of Critical Incidents*, and *SAGE Business Cases*.

Dana Schwieger is a Professor of Management Information Systems in the Harrison College of Business and Computing at Southeast Missouri State University. She holds a Ph.D. in Management Information Systems from Southern Illinois University–Carbondale. Her research interests include information systems liability, adaptive structuration theory, healthcare management information systems, teaching cases, and MIS curricula restructuring. She has published in *Information Systems Education Journal*, *Journal of Case Studies*, *Journal of Critical Incidents*, and *SAGE Business Cases*.

APPENDICES

Appendix A. Marx's 29 Questions

A. The Means

1. **Harm:** Does the technique cause unwarranted physical or psychological harm?
2. **Boundary**: Does the technique cross a personal boundary without permission (whether involving coercion or deception or a body, relational, or spatial border)?
3. **Trust:** Does the technique violate assumptions that are made about how personal information will be treated, such as no secret recordings?
4. **Personal relationships:** Is the tactic applied in a personal or impersonal setting?
5. **Invalidity:** Does the technique produce invalid results?

B. The Data Collection Context

6. **Awareness**: Are individuals aware that personal information is being collected, who seeks it, and why?
7. **Consent:** Do individuals consent to the data collection?
8. **Golden rule:** Would those responsible for the surveillance (both the decision to apply it and its actual application) agree to be its subject under the conditions in which they apply it to others?
9. **Minimization:** Does a principle of minimization apply?
10. **Public decision-making:** Was the decision to use a tactic arrived at through some public discussion and decision-making process?
11. **Human review:** Is there human review of machine-generated results?
12. **Right of inspection:** Are people aware of the findings and how they were created?
13. **Right to challenge and express a grievance**: Are there procedures for challenging the results, or for entering alternative data or interpretations into the record?
14. **Redress and sanctions:** If the individual has been treated unfairly and procedures violated, are there appropriate means of redress? Are there means for discovering violations and penalties to encourage responsible surveillant behavior?
15. **Adequate data stewardship and protection:** Can the security of the data be adequately protected?
16. **Equality-inequality regarding availability and application:** (a) Is the means widely available or restricted to only the most wealthy, powerful, or technologically sophisticated? (b) Within a setting, is the tactic applied broadly to all people, or only to those less powerful or unable to resist? (c) If there are means of resisting the provision of personal information are these means equally available, or restricted to the most privileged?
17. **The symbolic meaning of a method:** What does the use of a method communicate more generally?
18. **The creation of unwanted precedents:** Is it likely to create precedents that will lead to its application in undesirable ways?
19. **Negative effects on surveillants and third parties:** Are there negative effects on those beyond the subject and, if so, can they be adequately mediated?

C. Uses

20. **Beneficiary:** Does application of the tactic serve broad community goals, the goals of the object of surveillance, or the personal goals of the data collector?
21. **Proportionality:** Is there an appropriate balance between the importance of the goal and the cost of the means?
22. **Alternative means:** Are other, less costly means available?
23. **Consequences of inaction:** Where the means are very costly, what are the consequences of taking no surveillance action?
24. **Protections:** Are adequate steps taken to minimize costs and risk?
25. **Appropriate vs. inappropriate goals:** Are the goals of the data collection legitimate?
26. **The goodness of fit between the means and the goal:** Is there a clear link between the information collected and the goal sought?

27. **Information used for original vs. other unrelated purposes**: Is the personal information used for the reasons offered for its collection and for which consent may have been given, and do the data stay with the original collector, or do they migrate elsewhere?
28. **Failure to share secondary gains from the information:** Is the personal data collected used for profit without permission from, or benefit to, the person who provided it?
29. **Unfair disadvantage:** Is the information used in such a way as to cause unwarranted harm or disadvantage to its subject? (Marx, 1998)

Appendix B. ACM Code of Ethics

The Association of Computing Machinery's (ACM) Code of Ethics and Professional Conduct should serve as a guide for current, and future, computing practitioners. The Code, found at https://www.acm.org/code-of-ethics, is divided into four main sections: (1) General Ethical Principles, (2) Professional Responsibilities, (3) Professional Leadership Principles, and (4) Compliance with the Code (ACM, 2018; p. 1). Although upholding privacy and data security are woven throughout the document, Section 1 (General Ethical Principles) most obviously addresses the issue of privacy with five of its seven subsections related to the topic.

1.1 Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing: The focus of this subsection centers upon looking out for others. The subsection notes, "This principle, which concerns the quality of life of all people, affirms an obligation of computing professionals, both individually and collectively, to use their skills for the benefit of society, its members, and the environment surrounding them. This obligation includes promoting fundamental human rights and protecting each individual's right to autonomy. An essential aim of computing professionals is to minimize negative consequences of computing, including threats to health, safety, personal security, and privacy. When the interests of multiple groups conflict, the needs of those less advantaged should be given increased attention and priority" (ACM, 2018; p. 1).

1.2 Avoid Harm: This subsection of ACM's Code of Ethics addresses user privacy, and the responsibility of a computing professional, most substantially. "In this document, "harm" means negative consequences, especially when those consequences are significant and unjust. Examples of harm include unjustified physical or mental injury, unjustified destruction or disclosure of information, and unjustified damage to property, reputation, and the environment. This list is not exhaustive. Well-intended actions, including those that accomplish assigned duties, may lead to harm" (ACM, 2018; p. 1).

1.3 Be honest and trustworthy: The focus of this subsection centers upon the disclosure of system and personal capabilities to employers. Although this subsection does not address user privacy directly, the subsection emphasizes the importance of being honest and trustworthy in action and deed. "Honesty is an essential component of trustworthiness. A computing professional should be transparent and provide full disclosure of all pertinent system capabilities, limitations, and potential problems to the appropriate parties. Making deliberately false or misleading claims, fabricating or falsifying data, offering or accepting bribes, and other dishonest conduct are violations of the Code" (ACM, 2018; p. 1).

1.4 Be fair and take action not to discriminate: This subsection emphasizes the importance of fairness and equity in the profession: "the values of equality, tolerance, respect for others, and justice govern this principle. Fairness requires that even careful decision-making processes provide an avenue for the redress of grievances. Computing professionals should foster fair participation of all people, including those of underrepresented groups. Prejudicial discrimination on the basis of age, color, disability, ethnicity, family status, gender identity, labor union membership, military status, nationality, race, religion or belief, sex, sexual orientation, or any other inappropriate factor is an explicit violation of the Code. Harassment, including sexual harassment, bullying, and other abuses of power and authority, is a form of discrimination that, amongst other harms, limits fair access to the virtual and physical spaces where such harassment takes place" (ACM, 2018; p. 1).

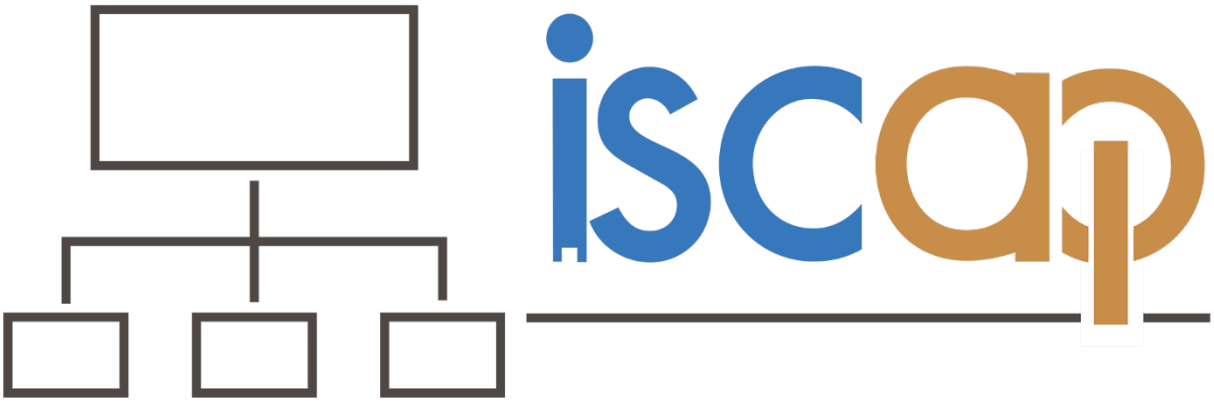
1.5 Respect the work required to produce new ideas, inventions, creative works, and computing artifacts: "Developing new ideas, inventions, creative works, and computing artifacts creates value for society, and those who expend this effort should expect to gain value from their work", is key in this subsection. "Computing professionals should therefore credit the creators of ideas, inventions, work, and artifacts, and respect copyrights, patents, trade secrets, license agreements, and other methods of protecting authors' works. Both custom and the law recognize that some exceptions to a creator's control of a work are necessary for the public good. Computing professionals should not unduly oppose reasonable uses of their intellectual works. Efforts to help others by contributing time and energy to

projects that help society illustrate a positive aspect of this principle. Such efforts include free and open-source software and work put into the public domain. Computing professionals should not claim private ownership of work that they or others have shared as public resources" (ACM, 2018; p. 1).

1.6 Respect privacy: This subsection of the document reminds professionals that "Technology enables the collection, monitoring, and exchange of personal information quickly, inexpensively, and often without the knowledge of the people affected." and encourages professionals to become familiar with the "…various definitions and forms of privacy and should understand the rights and responsibilities associated with the collection and use of personal information" (ACM, 2018; p. 1).

1.7 Honor confidentiality: The General Ethics Principles section wraps up with this subsection that reinforces the importance of privacy. "Computing professionals are often entrusted with confidential information such as trade secrets, client data… Computing professionals should protect confidentiality…" (ACM, 2018; p. 1).

INFORMATION SYSTEMS & COMPUTING ACADEMIC PROFESSIONALS



STATEMENT OF PEER REVIEW INTEGRITY

All papers published in the ***Journal of Information Systems Education*** have undergone rigorous peer review. This includes an initial editor screening and double-blind refereeing by three or more expert referees.

ISSN: 2574-3872 (Online) 1055-3096 (Print)