Privacy Under Pressure: Assessing Online Commercial Surveillance Countermeasures and Gaps

Christian Preti[1], Nicholas B. Harrell[2] and Alexander Master[2]
[1]United States Military Academy, West Point, USA
[2]Army Cyber Institute, West Point, USA

christian.preti@westpoint.edu
nicholas.harrell@westpoint.edu
alexander.master@westpoint.edu

Abstract: Ubiquitous technical surveillance is reshaping the modern information environment. Commercial web-tracking technologies have evolved into a pervasive technical surveillance infrastructure, enabling the large-scale collection of data from everyday activities as people participate in modern society. With sufficient analysis, this data can reveal sensitive information - posing risks to individuals, organizations, and national security. Several software packages exist to limit the exposure of personal information collected online. In recent years, laws and regulations, such as the GDPR and CCPA, have been implemented to help users protect their personal information, with varying degrees of success. This paper examines the recent scholarly literature on web tracking and commercial surveillance techniques. We then synthesize these studies to outline the methods that enable large-scale commercial surveillance on the Internet. Then, we analyze countermeasures designed to limit commercial data exposure, specifically assessing their effectiveness, technical constraints, and operational challenges. Our analysis reveals gaps in existing countermeasures and identifies opportunities for both technical and policy-based improvements to mitigate vulnerabilities introduced by commercially available information. These findings clarify the limitations of current web browser defenses and provide researchers and policymakers with directions on where further effort and investment are most needed.

Keywords: Commercial digital surveillance, Countermeasures, Data collection, Web tracking

1. Introduction

Digital Force Protection (DFP) has emerged as a critical component of operations security (OPSEC) for military personnel in an increasingly data-driven, global information environment (Shipp, 2026). Ubiquitous Technical Surveillance (UTS)[1] is a phenomenon in which data is continually collected about everyone. Data is derived from smartphone usage, purchases at retail locations, security cameras, Internet web browsing, and many other touchpoints of daily life in modern society. These data are often collected for the purpose of serving targeted advertising to consumers and increasing corporate profits. The data itself has become marketable; commercial data brokers buy, aggregate, and sell personally identifiable information (PII) about people without their consent or knowledge (Sherman, 2021). Researchers have shown how commercially available information (CAI), such as the data provided by data brokers, can be exploited with the potential for economic, psychological, and even physical harm to those targeted (GAO, 2025; Fox, 2024; Dawson & Matthew, 2024). CAI poses threats to force protection and OPSEC, as it can enable adversaries to identify, profile, and target service members and their families without requiring resources that were formerly held only by nation-state intelligence services.

The risks of aggregated CAI are not theoretical: for as little as $0.12 per record, foreign adversaries can acquire detailed personal information of active-duty U.S. service members from commercial data brokers with minimal verification or scrutiny (Sherman et al., 2023). This statement is based on a study conducted at Duke University, where the researchers purchased data sets containing information about 30,000 active-duty military members, including names, residential addresses, email addresses, health conditions, financial information, and religious affiliations, from three U.S. data brokers with little or no identity verification. A companion report by the Army Cyber Institute (ACI) examines the processes by which data enters the commercial ecosystem. The report found that data acquisition can involve tracking pixels on military-affiliated websites, identity verification tools such as ID.me (which offer discounts to military members), and third-party cookies that monitor users' online activity (Fox et al., 2023). An example case study was the ACI's examination of shopmyexchange.com, the online retail store operated by the Army and Air Force Exchange Service. There, the researchers found 22 ad trackers, 14 third-party cookies, keystroke loggers, and browser fingerprinting tools, which collectively transmit users' personal data to the commercial sector. If online services that cater directly to military members and their families have this amount of advertising technology (AdTech) embedded in their services, even service members

[1]The U.S. Federal Bureau of Investigation (FBI) defines UTS as the widespread collection of data and application of analytic methodologies for the purpose of connecting people to things, events, or locations (FBI, 2025).

who attempt to maintain small digital profiles and practice appropriate OPSEC in their personal lives will risk exposure through CAI.

The Duke data broker study demonstrates how consumer data can be easily extracted, packaged, and sold online (Fox et al., 2023). Although the tools threat actors use to gather data are unknown, a correlation between advertising techniques and clusters of PII can be identified. Even when utilizing privacy-preserving technologies, such as a virtual private network (VPN), browser data can be exploited if the victim irresponsibly enters their PII or fails to understand the digital surveillance environment.

The focus of this paper is on browser-based collection mechanisms, which are the front end of the data pipeline, and on the effectiveness of countermeasures, if any, against commercial digital surveillance. We offer a synthesis of recent literature on commercial web tracking to identify the browser-based mechanisms most likely to contribute to the data broker pipeline. We also assess the countermeasures publicly available to an average user, such as browsers, extensions, privacy settings, and DNS-based filtering, for their effectiveness against surveillance threats. Some of the findings highlight potential gaps, including the lack of countermeasures against server-side tracking, cross-site identity linking, and behavioral inference from metadata. Some countermeasures have usability challenges and cause browser anomalies, which, counterintuitively, increase users' identifiability. These findings have significant implications for service members and users operating in high-risk environments, especially regarding the information accessible to online malign actors. This paper is a structured narrative synthesis of recent literature rather than a systematic review; its aim is to identify practical gaps and generate hypotheses for future empirical work.

2. Background

Extensive data collection online has been ongoing for several years, primarily for targeted advertising. Specifically, these “Web tracking systems…automatically record data and behaviors of Internet users,” and are crucial for “marketing and advertising strategies;” however, they “pose a threat to individual privacy rights” as “users often lack awareness” of the extent to which their data is collected (Tasoulas, Gazis, and Tsohou, 2025). The lack of user awareness poses concerns for everyday users, especially when combined with the vast array of digital surveillance technologies currently in use. This threat applies particularly to service members, whose PII can be exploited if acquired by malign actors. For example, “commercial data brokerage services expose[d] location data of service members and use[d] it to follow them from their residences to sensitive facilities, such as intelligence organizations or nuclear sites around Europe” (Master et al., 2025). Data gathered online contributed to this exposure, but it stems from an issue on the Internet that every user experiences: a lack of transparency about how their data is collected and what can be done to limit this process.

2.1 Related Work

From our literature analysis, several patterns emerge in research on commercial internet surveillance. The taxonomy of internet surveillance techniques by Gazis, Tasoulas, and Tsohou (2025) divides the subject into four primary categories: HTTP Tracking, API Tracking, User Identification, and Complex Tracking.

The first category, HTTP Tracking, involves collecting personal data from internet users via the HTTP protocol, including cookies, web beacons, and email tracking. In the literature, cookies have been shown to be effective for large-scale, passive tracking of internet users, often without their knowledge, for clustering identities and profiling them over the long term (Englehardt et al., 2015). Although first-party cookies have been proven to be helpful in the provision of Internet services, third-party cookies and the use of tracking pixels have been identified as a major privacy concern to the Internet and its users (Ourrahte, El-Yahyaoui, and Ziani, 2025). Despite web browsers broadly moving to block third-party cookies,[2] server-side and scriptless methods, such as those using tracking pixels, can still be used for session and configuration inference (El Hajj Chehade, Stock, and Troncoso, 2025).

API and storage-based internet tracking techniques have been found to be effective in the collection of the personal data of internet users, including the use of Flash cookies, HTML5 local and session storage, and the so-called “evercookies” that have the ability to regenerate their IDs even after being deleted by the internet users (Tasoulas, Gazis, and Tsohou, 2025).

[2] Google Chrome is a notable exception; see (Chavez, 2024) and (Leith, 2021). While Alphabet originally intended to block third-party cookies in Chrome, the company abandoned the effort in 2024.

Another avenue that enhances tracking persistence is the use of user identification techniques. These techniques involve creating fingerprints from system-level attributes. Techniques such as canvas fingerprinting and cookie synchronization enable unique identification of individuals without the need for traditional cookies (Ourrahte, El-Yahyaoui, and Ziani, 2025). The literature has highlighted the challenges users face in identifying and mitigating fingerprinting techniques, given that these techniques provide minimal evidence of tracking (Kaur et al., 2017). Recent studies in the field suggest that fingerprinting techniques can also exploit interactions users have with countermeasures; for example, Solomos et al. (2022) demonstrated the ability to fingerprint browsers using extensions, thereby undermining the effectiveness of many countermeasures.

Other sophisticated tracking methods often include integrating HTTP tracking, storage-based identifiers, fingerprinting, and behavioral tracking. These tracking methods are often associated with robust data infrastructures and the use of machine learning capabilities. These tracking methods are often used for in-depth analytics, cross-site user linkage, and behavioral analysis (Tasoulas, Gazis, and Tsohou, 2025). Behavioral tracking methods, such as keystroke tracking, have been used to extend tracking capabilities to include sensitive user information in malware-related tracking (Baek et al., 2012). Recent studies have indicated the extension of tracking to cellular networks and mobile devices. In this case, fingerprinting tracking methods have been used to track application usage, geolocation, and inter-user relationships within the same network cell (Baek, 2023). This can be detrimental to OPSEC because users often access the Internet using personal devices rather than enterprise equipment with network or browser-based mitigations in place.

3. Methodology

Focusing specifically on the data types revealed by service members in the Duke paper, our research question becomes: “How do commercially available data sources enable the aggregation of service members’ personally identifiable information, and what gaps in existing countermeasures allow this exposure to persist?” Research has been completed on several surveillance countermeasures and their effectiveness (such as the work completed by Bujlow et al.; Ourrahte, El-Yahyaoui, and Ziani; Englehardt et al.; and Luangmaneerote, Zaluska, and Carr). However, the application to service members is underexplored. First, we survey the literature for studies of commercial digital surveillance technologies. Papers were sourced from OpenAlex, Semantic Scholar, and Scopus, with a supplementary Google Scholar search for existing systematic reviews. Two parallel search streams covered tracking mechanisms (2015–2026) and countermeasures (1995–2026), excluding physical surveillance, non-English publications, and non-peer-reviewed sources. Of 3,060 initial records, 262 duplicates were removed, and the remaining 2,798 were screened by title and abstract; 39 candidates advanced to full-text review, yielding a final corpus of 15 studies. Additional sources were identified through citation chasing, reflecting the fragmented publication landscape of web-tracking defense research across security conferences, journals, and government reports.

Then, we synthesize the effectiveness of various countermeasures, highlighting gaps that threaten service members and OPSEC. Additionally, the overall impacts of a lack of information regarding digital surveillance (along with the current countermeasures) are analyzed.

The synthesis was also intended to explore the extent to which data have already been collected about service members. As seen in Fox et al.’s report (2023), several datasets of active-duty personnel were collected from data brokers at “at low cost, by domestic or foreign entities” (including information such as “[n]ame, home address, email,” and other information on around 5,000 personnel). This vast data collection, when combined with the primary methods of digital surveillance and the leading countermeasures, will provide the foundation for recommendations on future policy and further research.

We first classify the primary digital surveillance technologies (namely, cookies, tracking pixels, fingerprinting, behavioral methods, and cross-device methods). Then, we analyze the gaps that remain to offer recommendations for further research and development of countermeasures.

4. Survey

4.1 Cookies

Cookies themselves act as an “identifier” within a website’s database and will “store user data, such as passwords” with the overall goal of convenience (Tasoulas, Gazis, and Tsohou, 2025). Websites typically use first-party cookies to improve overall functionality, with the user’s experience in mind. These cookies are not primarily a privacy concern, as they are tied to the specific website the user intended to visit; the responsibility

falls on both the user and the website owner to ensure that both parties understand the services being provided. However, the issue becomes apparent with the introduction of third-party cookies.

4.1.1 Third-party cookies

The "presence of multiple unrelated third-party cookies on most web pages, albeit pseudonymous, can tie together most of a user's web traffic without having to rely on IP addresses" or other surveillance techniques (Englehardt et al., 2015). This issue extends beyond the third-party as well, as "many web pages reveal an already logged-in user's identity in plaintext. Thus, an adversary that can wiretap the network can not only cluster together the web pages visited by a user but can then attach real-world identities to those clusters" (Englehardt et al., 2015). This is especially threatening to OPSEC. Adversaries—in order "[t]o link users across different networks and over time"—will "utilize…third-party unique cookies assigned to browser instances by websites" that allows adversaries to "accumulate browsing statistics through many different websites" (Englehardt et al., 2015; Bujlow et al., 2017). PII is within reach of any threat actor, making third-party cookies a worrying threat to privacy.

4.1.2 Persistent cookies

In conjunction with third-party cookies, persistent cookies are more difficult for users to delete. They "track users over a long period," "remain[ing] on the device even if you close the browser" which makes them especially dangerous (Ourrahte, El-Yahyaoui, and Ziani, 2025). In the purpose of this paper, this section will also include other versions of advanced cookies—including zombie cookies and evercookies, which are "highly advanced tracking techniques…to leave tracking in place, even if a user tries to delete them"—as they all are more dangerous than basic third-party cookies (Ourrahte, El-Yahyaoui, and Ziani, 2025). While third-party cookies primarily track users for advertising purposes, other forms of cookies are more effective at tracking users for harmful intent. Additionally, these persistent cookies can be "controlled by scripts," allowing a threat actor with a clear target to passively attack anyone (Tasoulas, Gazis, and Tsohou, 2025).

4.2 Tracking Pixels

Another prevalent tool used for both advertising and surveillance is a tracking pixel.[3] These are "small pieces of embedded code that transmit user data to external vendors," and these propose a high risk to personal information as they "collect, transmit, and potentially expose sensitive…information to external entities" (Atasoy, McDonough, and Zhang, 2025). Although these can be protected against with browsers, they "operate server-side, making them harder to detect and block" while also "becom[ing] a dominant tracking tool for measuring user engagement" (Atasoy, McDonough, and Zhang, 2025). These three researchers found "a critical regulatory gap in healthcare privacy, as tracking pixels operate outside the traditional scope of Health Insurance Portability and Accountability Act protections" (2025). This gap is explained within an article from Huo, Bland, and Levchenko, in which they "discovered that 14% of 465 [medical] systems…leak[ed] some form of protected health information to third-party services…including laboratory test results, phone numbers, patient names, emails," and more (2022). This is directly comparable to the threats proposed in this paper, as the disclosure of service member's PII by threat actors through tracking pixels offers an avenue to secretly record information.

4.3 Fingerprinting

Fingerprinting describes the "technique used to create a unique string that identifies internet users" which "is stored in a cookie or browser storage, allowing websites to request it and identify visitors" (Tasoulas, Gazis, and Tsohou, 2025). However, it does not necessarily need cookies; it is also able to "rel[y] on information obtained from the user's browser and device," making them extremely difficult to avoid (Ourrahte, El-Yahyaoui, and Ziani, 2025). This goes beyond cookies, as threat actors develop profiles that—in the best case—"provide personalized services," while—in the worst case—collect vast amounts of PII about someone through "the unique pattern of information visible whenever a computer visits a website" (Tasoulas, Gazis, and Tsohou, 2025; Kaur et al., 2017). Examples include "Canvas, Browser, HTTP Headers, Battery, IP Address," and others; all of these rely on characteristics unique to the user accessing the internet and range from digital components (i.e. browser settings) to physical components (battery type).

These are especially concerning because they can allow threat actors to map users across websites, as persistent cookies do. Additionally, knowledge of a user's component version can lead to the exploitation of vulnerabilities

[3]Tracking pixels are sometimes also referred to as web beacons.

specific to that version. In the context of OPSEC, as outlined in the cookies section, threat actors can build profiles of service members by leveraging data service members use to access the Internet without their awareness.

4.4 Behavioral Methods

Other methods focus on analyzing specific user behaviors. For example, spyware— "software programs installed on a computer to monitor activity or cause harm"—will "often collaborate with other software or techniques, such as Adware or keystroke loggers" (which can "capture sensitive information like passwords") (Tasoulas, Gazis, and Tsohou, 2025). Unlike the methods described previously, surveillance technologies analyze user behavior and actions to monitor trends and gather data. This includes a plethora of various techniques, but for the purpose of this paper, we will broadly generalize the human element. This is fully shown in Bella et al.'s "A Socio-Technical Methodology for the Security and Privacy Analysis of Services," which breaks surveillance technologies into "layers" and introduces the human element as an important level for future research to understand the human impact on digital surveillance (2014). Additionally, the paper argues that "an extended view of a security protocol is needed to include human users, social protocols, and behaviors; that is, see the system as a much more complex socio-technical system" (Bella et al., 2014).

This argument posits that humans are the most vulnerable aspect of digital security, with PII gathered to target users based on their specific behavior. This can include data gathered from other digital surveillance techniques (cookies, fingerprints, etc.), but they can also include behavioral surveillance techniques such as keystroke logging, "bidding history," "shopping preferences," "[m]ouse click and movement analysis," or other PII "in context-aware phishing" (Bella et al., 2014; Ourrahte, El-Yahyaoui, and Ziani, 2025). Logging information while analyzing the human element emphasizes the need for education on proper internet usage, especially for service members. Behavioral surveillance techniques only increase the opportunities for threat actors to gather PII, posing a risk to users and servicemembers alike.

4.5 Cross-device Methods

Cross-device methods address a real threat that has become increasingly prevalent with cellular devices. The possibility of threat actors targeting users through the victim's phone is another category of digital surveillance techniques. Within Baek et al.'s "Targeted Privacy Attacks by Fingerprinting Mobile Apps in LTE Radio Layer," the researchers "demonstrate[d] that the physical channel of LTE alone is sufficient to carry out previously-proposed privacy attacks to identify which mobile applications are in use on a device," which "can be carried out through self-deployed sniffers directly on the exact traffic transmitted in the air…to…detect communication links between targeted users" (2023). Although this technique uses fingerprinting (and is worrisome because it employs "undetectable techniques"), it warrants a specific classification because it represents the development of adversarial techniques used by threat actors against users' cellular devices (Baek et al., 2023). As more people continue to purchase and use smartphones, this presents a new opportunity for an adversary to exploit vulnerabilities in their wireless capabilities.

This surveillance technique also has implications for service members. Digital phones could disclose PII if a threat actor detected communication links or connected to the LTE channel the victim was on. Of course, this does not argue for service members to refrain from cell phone usage. Instead, it ties directly to a future research recommendation in "Tracking the Trackers: Commercial Surveillance Occurring on U.S. Army Networks," where the authors stated that "[d]evices such as smartphones utilize commercial cellular providers to connect to Internet resources, and do not benefit from DoDIN security;" therefore, methods should be imposed to protect service members digital devices to ensure threat actors do not take advantage of them (2025).

5. Synthesis

We now outline the different categories of countermeasures to digital surveillance technologies currently available, along with their effects and capabilities. Additionally, the limitations and gaps are analyzed to determine the drawbacks of each and their overall effectiveness. The findings are summarized in Table 1, which is used to graphically represent the synthesis. Additionally, the categories will be modeled after the research conducted in Ourrahte, El-Yahyaoui, and Ziani's "Exploring Techniques and Countermeasures Against Browser Tracking: A Comprehensive Survey" (2025) to group similar technologies and aggregate data.

Table 1: Synthesis of Countermeasures to Digital Surveillance Technologies

Category	Examples	Usage (against)	Gaps	Sources
Browsers	Tor Browser, Mullvad Browser, Brave Browser, Mozilla Firefox, Apple Safari	Cookies, tracking pixels, fingerprinting, cross-device identification	Reduced functionality of some websites, burden to users	Ourrahte, El-Yahyaoui, and Ziani, 2025; Luangmaneerote, Zaluska, and Carr, 2016
Browser extensions/plugins	Ghostery, uBlockOrigin, AdBlock Plus, NordVPN Extension	Cookies, tracking pixels, fingerprinting, advertisements	Blocks some content, increases processing time, added burden to users	Englehardt et al., 2015; Ourrahte, El-Yahyaoui, and Ziani, 2025
Domain Name System (DNS)	pfBlockerNG, NextDNS, PiHole	Tracker domain endpoints	Domains and IP addresses are often ephemeral	Master et al., 2025; Lin et al., 2022
Education	Organization-wide, Individual training	Behavioral	Requires user commitment and cognitive load	Fox et al., 2023
Policy/Regulatory	General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA)	Data collection, data sharing, data deletion	Varies by jurisdiction of regulated entities and which citizens are entitled to protections	Miller et al., 2024; Papadogiannakis et al., 2021

5.1 Browsers

A basic (but effective) way to protect against digital surveillance online is to use specific browsers. For example, Microsoft Edge allows users "to block trackers designed to monitor user behavior," "prevents tracking by blocking trackers from sites the user has not visited," and "can…block all tracking by activating [an] option;" however, it is not as robust as alternative browsers designed specifically with privacy implementations (Ourrahte, El-Yahyaoui, and Ziani, 2025). Other browsers, like Mozilla Firefox and Brave, have built-in mitigations for cross-site tracking, third-party cookies, and resistance to browser fingerprinting (Ourrahte, El-Yahyaoui, and Ziani, 2025). Additionally, there exist "[p]rivacy-focused search engines" that include DuckDuckGo, which "use some techniques to prevent forwarding the search results to the linked website" (typically through obfuscation) (Bujlow, 2017). Firefox also, by default, "is known for forbidding reading cookies by third parties" and offers several plugins/addons to enhance protection, such as RequestPolicy (which "blocks all the cross-site requests") and Lightbeam (which "enables the user to see the requests made to the first- and third-party sites") (Bujlow, 2017).

Another major browser committed to keeping the user secure is Tor. While investigating the effectiveness of countermeasures to fingerprinting, Luangmaneerote, Zaluska, and Carr (2016) found that Tor was very effective at preventing fingerprinting (2016). However, this came with some gaps that offered adverse effects to users. This included problems with "display, functionality, usage, and login problems," making it "appear to generate more user dissatisfaction than other techniques," as well as slower connection speeds. So, while certain protective browsers might be more effective at protecting user information, they may come at the cost of usability, potentially limiting their widespread adoption due to user frustration.

5.2 Browser Extensions/Plugins

Another primary countermeasure to digital surveillance technologies is the usage of browser extensions/plugins. These allow users to provide additional protection for their browser of choice, ensuring their data is further protected against threats. One example is "Ghostery…a popular list-based browser extension for blocking third-party requests to domains considered to be trackers" (Englehardt et al., 2015). This countermeasure was effective in a study by the authors of "Cookies That Give You Away: The Surveillance Implications of Web Tracking," which showed a statistically significant decrease in clustering via cookies (2015). Another similar plugin is uBlock Origin, which "[b]locks tracking scripts, ads, and intrusive domains" that is "[l]ightweight, open-

source, and highly configurable" (Ourrahte, El-Yahyaoui, and Ziani, 2025). However, despite these tools' effectiveness, users sometimes remain vulnerable, which can also cause user experience degradation on some websites. These extensions attempt to block data collection, but rely on data feeds of known third-party endpoint domains to function. As new tracker domains are introduced (or large advertising firms change their tracker domains to avoid blocking tools), users experience gaps in coverage.

This solution still does "offer tools for blocking trackers, encrypting data, or masking IP addresses and other information" to protect user data online (Ourrahte, El-Yahyaoui, and Ziani, 2025). However, user experience degradation may prevent adoption of such tools. Ad blocking extensions may "slow down browsing," cause extra effort to use (from users), "block some useful content," "slow down your connection," and be incompatible with certain websites (Ourrahte, El-Yahyaoui, and Ziani, 2025). Although these add extra burdens to users, they can still reduce the likelihood of a PII breach. Additionally, both browsers and browser extensions/plugins can be installed on cellular devices, further protecting phones and user data.

5.3 Domain Name System (DNS)

From the user standpoint, it is possible to block the advertising servers that deliver content directly to devices and web browsers. DNS-based ad-blocking tools such as Pi-hole (Pi-hole LLC, 2024), pfBlockerNG (Nguyen, 2024), and NextDNS (NextDNS, 2024) operate as DNS sinkholes, intercepting DNS queries for known tracker and advertising domains before a connection is established and returning a non-routable address in place of the tracker endpoint (Master et al., 2025). Because blocking occurs at the network layer before any data exchange, these tools can protect all devices on a network, regardless of operating system or browser, including smart TVs, mobile devices, and IoT devices that cannot run browser-level extensions (Pi-hole LLC, 2024). While DNS-based ad blocking is very effective, it requires users or organizations to create access lists that block specific domains. The IP addresses and domain names of ad and tracker servers may change over time, requiring configuration adjustments.

The effectiveness of DNS-based blocking depends on the currency and coverage of upstream blocklists, which aggregate known advertising and tracking domains from community-maintained sources such as EasyList and EasyPrivacy. Lin et al. (2022) demonstrate this requirement as a structural vulnerability rather than a routine maintenance burden. After conducting a crawl of 50,000 websites, Lin et al. (2022) show that advertisers systematically register replica ad domains that evade filter lists. Many users remained exposed for over two years despite having DNS-based blocking enabled.

5.4 Education

Another countermeasure exists beyond software or even applications. This section primarily focuses on preventing digital surveillance by raising users' awareness through simple education to counter the "socio-technical" surveillance described in behavioral methods for digital surveillance. As many of these surveillance techniques are passive and rely on unaware users, proper training on these topics will help users develop the online skills necessary to use the Internet safely.

ACI has also emphasized this need for education, especially among military service members. For example, while analyzing the commercial surveillance occurring within U.S. Army Networks, recommendations were proposed to "[e]ducate service members and civilian employees about the risks posed by commercial tracking, CAI (commercially available information), and data brokers" (Master et al., 2025). This directly ties into the data brokers mentioned within Sherman et al., 2023, where it is recommended that "[t]he Army should provide awareness training and best practices surrounding commercial data collection" at the institutional level (as, although individual training is helpful, it is not always fully enforced as it relies upon the responsibility of the individual much more heavily).

6. Discussion and Conclusion

The literature reveals that the primary design goal of surveillance architectures is to externalize the processes of data collection and identity resolution, effectively limiting the visibility of the aggregation of session data, metadata, and behavioral data post-transmission. While countermeasures implemented on the client-side may effectively limit the visibility of tracking signals, they do not limit session aggregation, probabilistic identity resolution, or long-term profile construction on the server-side. Thus, the effectiveness of countermeasures is inherently limited, regardless of proper implementation.

The above findings are particularly relevant to OPSEC. The findings of the Duke study reveal that the information present in the commercially available datasets is already sufficiently rich to enable the identification, clustering,

and profiling of service members without access to classified systems or government networks. The findings of the above studies, in combination with the literature on tracking pixels, fingerprinting, and behavioral inference, reveal that the issue of exposure is not simply the result of the presence of unique identifiers, but rather the result of the aggregation of impermanent signals that, in combination, can be indicative of an individual's activities. The inability to view the aggregation mechanisms effectively limits the user's ability to properly assess risk, thereby making the risk mitigation process more complex.

Several studies suggest that the use of privacy-enhancing tools may have unintended effects. Configuration-based defenses, such as customized ad blockers or extension-rich browsers, may decrease population-level anonymity by making users more distinctive. This is important to service members who operate in high-risk environments. Efforts to minimize surveillance exposure may facilitate identity resolution when combined with server-side analytics, underscoring that individual-level countermeasures alone are not sufficient to achieve OPSEC-relevant risk reductions.

The overall body of evidence indicates that current countermeasures place the onus on the end user while ignoring the most significant means of digital surveillance. While education and awareness are important for reducing risk-taking behaviors, they are not enough to address the passive, opaque data flows associated with commercial infrastructures. This will require further research into server-side tracking behaviors and methods to reduce data collection, retention, and resale at the source.

Prevalent digital surveillance technologies and gaps in existing countermeasures underscore the need for expanded policy measures to protect users. Examples of existing policy include the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). The GDPR "obliges websites to seek users' consent before collecting their personal data," and "users must be informed if their data is stolen, and companies must protect their customers' data" (Ourrahte, El-Yahyaoui, and Ziani, 2025). This provides some protection to users in Europe. Current legal frameworks in the U.S. provide few avenues to limit or restrict data collection and are only at the individual state level rather than applied nationally. The CCPA is a law that governs the protection of online users' privacy and the processing of their data by companies, which allows users to "opt out" of the sale of their data (Ourrahte, El-Yahyaoui, and Ziani, 2025). This does not provide recourse after data has been collected, shared, or sold, and the exposure of PII through CAI persists despite California's efforts – and protections are only afforded to California residents. Policymakers should consider widely implementing "opt-in only" requirements when proposing consumer privacy legislation, to extend proactive protection to at-risk populations such as service members and their families. Users should be fully aware when first-party or third-party entities are collecting their sensitive personal information, and have the agency to reject such requests if they desire or must do so due to the sensitivity of their employment. Given that commercial entities can aggregate service members' PII, sell it to others, and profit from it – some of those customers potentially being malicious online actors – poses significant challenges for military members and government officials working in a national security context.

Acknowledgements

We would like to express our gratitude to the Army Cyber Institute for their financial support. We also thank our anonymous peer reviewers for their detailed and helpful feedback, which improved this manuscript's quality.

The analysis presented in this paper is attributable exclusively to the authors. It does not represent the views of the United States Military Academy nor imply or constitute endorsement by the U.S. Army or U.S. Government.

Ethics declaration: No IRB approval was required for this study.

AI declaration: We used Grammarly to correct spelling mistakes, identify grammar errors, and adjust awkward phrasing. We also used Semantic Scholar to find sources. Our use of artificial intelligence tools helped to refine our scope and focus of tracking technologies toward OPSEC and its application to service members; all conceptual content, analytical framing, and interpretation reflect the intellectual contribution and responsibility of the authors.

References

Atasoy, Hilal, McDonough, Ryan, and Zhang, Guangyue. (2025) "Beyond the click: Pixel tracking technologies and patient data security in hospitals," *PNAS Nexus, Vol. 4*. Available at: https://academic.oup.com/pnasnexus/article/4/12/pgaf360/8373188.

Baek, Jaejong et al. (2023) "Targeted Privacy Attacks by Fingerprinting Mobile Apps in LTE Radio Layer," *53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks*. Available at: https://sefcom.asu.edu/publications/jaejong-dsn23.pdf.

Bella, Giampaolo et al. (2014) "A Socio-Technical Methodology for the Security and Privacy Analysis of Services," *2014 IEEE 38th International Computer Software and Applications Conference Workshops*, Vasteras, Sweden. Available at: https://ieeexplore.ieee.org/document/6903163/authors#authors.

Bujlow, Tomasz et al. (2017) "A Survey on Web Tracking: Mechanisms, Implications, and Defenses," *Proceedings of the IEEE, 1558-2256 (electronic), vol. 105*. Available at: http://tomasz.bujlow.com/publications/2017_journal_ieee_survey_on_web_tracking.pdf.

Chavez, A. (2024) "A New Path for Privacy Sandbox on the Web", *Google Blog*. Available at: https://privacysandbox.google.com/blog/privacy-sandbox-update.

Chojnacki, B., Daher, Z. and Master, A. (2025) "Poster: Unseen threats: The privacy risks of data collection in government fleet vehicles", *3rd USENIX Symposium on Vehicle Security and Privacy*, Seattle, WA. Available at: https://www.usenix.org/conference/vehiclesec25/presentation/chojnacki-poster.

Dawson, J. and Matthew, K. (2024) "Data as Ammunition: A New Framework for Information Warfare", *The Cyber Defense Review*, 9(2), pp. 93–108. Available at: https://www.jstor.org/stable/48784777.

El Hajj Chehade, S., Stock, B. and Troncoso, C. (2025) "Double-edged shield: On the fingerprintability of customized ad blockers," In: Proceedings of the USENIX Security Symposium, USENIX Association.

Englehardt, Steven et al. (2015) "Cookies That Give You Away: The Surveillance Implications of Web Tracking," ACM Digital Library. Available at: https://dl.acm.org/doi/10.1145/2736277.2741679.

Federal Bureau of Investigation (FBI), Office of the Inspector General. (2025) *Audit of the Federal Bureau of Investigation's efforts to mitigate the effects of ubiquitous technical surveillance*, Report no. 25-065. Available at: https://oig.justice.gov/sites/default/files/reports/25-065_t.pdf.

Fox, J., Master, A., Starck, N. and Dawson, J. (2023) *Death By a Thousand Cuts: Commercial Data Risks to the Army*, Technical report, West Point, NY: Army Cyber Institute. Available at: https://hdl.handle.net/20.500.14216/1694.

Fox, J. (2024) "The New Insider Threat: How Commercially Available Data Can Be Used to Target and Persuade", *The Managing Insider Risk & Organizational Resilience (MIROR) Journal*, 2(1), pp. 61–86. Available at: https://hdl.handle.net/20.500.14216/1695.

Harrell, N., Master, A., Starck, N. and Eerhart, D. (2025) "Tactics and Techniques of Information Operations: Gaps in US Response to Counter Malign Influence", *International Conference on Cyber Warfare and Security (ICCWS)*. Available at: https://doi.org/10.34190/iccws.20.1.3271.

Huo, M., Bland, M. and Levchenko, K. (2022) "All Eyes On Me: Inside Third Party Trackers' Exfiltration of PHI from Healthcare Providers' Online Systems", *Proceedings of the 21st Workshop on Privacy in the Electronic Society*, Los Angeles, CA, USA, pp. 197–211. Available at: https://doi.org/10.1145/3559613.3563190.

Kaur, Navpreet et al. (2017) "Browser Fingerprinting as User Tracking Technology," *2017 11th International Conference on Intelligent Systems and Control (ISCO)*, Coimbatore, India. Available at: https://ieeexplore.ieee.org/document/7855963.

Leith, D.J. (2021) "Web Browser Privacy: What Do Browsers Say When They Phone Home?", *IEEE Access*, 9. Available at: https://doi.org/10.1109/ACCESS.2021.3065243.

Lin, Su-Chin et al. (2022) "Investigating Advertisers' Domain-changing Behaviors and Their Impacts on Ad-blocker Filter Lists", *Proceedings of the ACM Web Conference 2022*, Lyon, France (Virtual event), pp. 576–587. Available at: https://doi.org/10.1145/3485447.3512218.

Luangmaneerote, Sakchan, Zaluska, Ed and Carr, Leslie. (2016) "Survey of Existing Fingerprint Countermeasures," *2016 International Conference on Information Society (i-Society)*, Dublin, Ireland. Available at: https://ieeexplore.ieee.org/document/7854198.

Master, A., Fox, J., Starck, N., Love, M. and Allison, B. (2025) *Tracking the Trackers: Commercial Surveillance Occurring on U.S. Army Networks*, Technical report, West Point, NY: Army Cyber Institute. Available at: https://doi.org/10.48550/arXiv.2602.12388.

Master, A. (2023) *Modeling and Characterization of Internet Censorship Technologies*. Dissertation. Purdue University. Available at: https://doi.org/10.25394/PGS.23666784.

Miller, K., Lukic, S. and Skiera, B. (2024) "The Impact of the GDPR on Online Tracking." Available at: https://doi.org/10.48550/arXiv.2411.06862.

NextDNS. (2024) *The new firewall for the modern Internet*, NextDNS. Available at: https://nextdns.io.

Nguyen, B. (2024) *pfBlockerNG*, Netgate. Available at: https://docs.netgate.com/pfsense/en/latest/packages/pfblocker.html.

Ourrahte, Malak, El-Yahyaoui, Ahmed, and Ziani, Fatima-Ezzahra. (2025) "Exploring Techniques and Countermeasures Against Browser Tracking: A Comprehensive Survey," *2025 5th International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET)*, Fez, Morocco. Available at: https://ieeexplore.ieee.org/document/11008149.

Papadogiannakis, A., Ioannidis, S., and Polakis, I. (2021) "User Tracking in the Post-Cookie Era: How Websites Bypass GDPR Consent to Track Users". Available at: https://doi.org/10.48550/arXiv.2102.08779.

Pi-hole LLC. (2024) *Pi-hole: Network-wide ad blocking*, Pi-hole LLC. Available at: https://pi-hole.net.

Sherman, J. (2021) *Data brokers and sensitive data on U.S. individuals*, Duke University. Available at: https://techpolicy.sanford.duke.edu/wp-content/uploads/2021/08/Data-Brokers-and-Sensitive-Data-on-US-Individuals-Sherman-2021.pdf.

Sherman, J., Barton, H., Klein, A., Kruse, B. and Srinivasan, A. (2023) Data Brokers and the Sale of Data on U.S. Military Personnel: Risks to Privacy, Safety, and National Security. Durham, NC: Duke University Sanford School of Public Policy. Available at: https://techpolicy.sanford.duke.edu/data-brokers-and-the-sale-of-data-on-us-military-personnel.

Shipp, J.W. (2026) "Digital force protection for expeditionary land forces: An early-warning framework for mission command resilience," *The Cyber Defense Review*, 11(1), pp. 111–126. Available at: https://doi.org/10.55682/cdr/vcg8-sh28.

Solomos, K. et al. (2022) The dangers of human touch: Fingerprinting browser extensions through user actions, In: Proceedings of the 31st USENIX Security Symposium, 10–12 August 2022, Boston, MA, USA, USENIX Association, pp. 717–733.

Tasoulas, T., Gazis, A. and Tsohou, A. (2025) *Comprehensive classification of web tracking systems: Technological in-sights and analysis*. Available at: https://doi.org/10.48550/arXiv.2504.13922.

U.S. Government Accountability Office (GAO) (2022) *Information environment: Opportunities and threats to DOD's national security mission*. Report, GAO-22-104714. Available at: https://www.gao.gov/products/gao-22-104714.

U.S. Government Accountability Office (GAO) (2025) *Information Environment: DOD Needs to Address Security Risks of Publicly Accessible Information*. Available at: https://www.gao.gov/products/gao-26-107492.

Yu, Z., Macbeth, S., Modi, K. and Pujol, J.M. (2016) "Tracking the Trackers", *Proceedings of the 25th International Conference on World Wide Web*, Montréal, Québec, Canada. Available at: https://dl.acm.org/doi/10.1145/2872427.2883028.