History repeats itself: Studying the Evolution of an Immigration Surveillance App in the United States from 2021 to 2025

Kentrell Owens
Max Planck Institute for Security and Privacy
kentrell.owens@mpi-sp.org

***Abstract*—While much attention has been given recently to Immigration and Customs Enforcement (ICE), the treatment of the people detained by ICE, and the treatment of those who protest ICE's actions, less attention has been given to exactly how ICE locates and tracks the people it targets. They do this, in part, through an immigration surveillance app (SmartLINK) that many migrants are required to installed on their phones. Migrants that have SmartLINK installed on their phones have their location tracked and must do "check-ins" that use face and voice recognition at random times. This app was developed for ICE by a private contractor, BI, in 2018.**

There are publicly-available documents (e.g., contracts) describing how the app *should* behave, but it is unclear if SmartLINK currently complies with these terms or if there have been incidents of non-compliance in the past. Given the sensitive nature of the data collected by this app and the fact that it is developed by a government contractor, there is an opportunity to conduct a technical audit of the app that (similar to tax audits) includes historical records to evaluate contractual and regulatory compliance. To this end, we propose a retrospective, technical analysis of SmartLINK and relevant public records to answer, to the extent possible: has BI been transparent and honest—currently and historically—about the data practices of SmartLINK?

1. Introduction

When people apply for asylum in the US or have an initial encounter with ICE within the US (e.g., while having an expired visa), they often have to install a smartphone app (SmartLINK) that tracks their location and collects biometrics (i.e., face and voice data) during in-app check-ins [1]–[5]. According to the latest numbers reported by ICE from February 2026, 135,279 people are required to use this app, for an average of 865 days [6].

As of January 2026, Immigration and Customs Enforcement (ICE) is the largest law enforcement agency in the United States, with a budget larger that the FBI, the Federal Bureau of Prisons, and the militaries of most countries in the world [7]. In September 2025, GEO Group—the parent company of BI and largest private prison company in the U.S.—was awarded a two-year contract (estimated to cost 121 million USD) by ICE to continue its management of the program that administers SmartLINK [8], [9]. In addition to maintaining the SmartLINK app, BI also has "case specialists" that provide case managements services—making them functionally private parole officers for migrants.

Given the amount of public money and power delegated to BI and the potential harm resulting from misreported data practices or negligence, we propose a technical audit of BI's SmartLINK app and its data practices. While there has been work analyzing people's experiences using SmartLINK [10], [11] and some high-level technical analysis on a specific version of the app [12], we lack insight into how this app has evolved over time, how these changes may have reflected shifts in its data practices, and if they contradicted its stated behavior at the time that these changes were implemented.

1.1. A motivating example

ICE has insisted that SmartLINK only tracks people using the app during their check-ins and not continuously in the background [13]. ICE's FAQ page for SmartLINK poses the question ("Does BI SmartLINK have persistent location tracking capabilities?"), and answers it by stating that "BI SmartLINK **is not capable** of persistent tracking when loaded on a participant provided device" [13]. [1] This statement was true for the SmartLINK APK from July 2023, because the app did not have the permission required to read the background location data (android.permission.ACCESS_BACKGROUND_LOCATION). However, this permission was present in the April 2025 APK, and ICE's FAQ has not been updated to reflect that the capability now exists. While we stress that this capability does not directly imply *use* of this permission, it does indicate a change in SmartLINK that invalidate previous statements regarding its data practices.

1.2. Our proposal

A longitudinal analysis could help us understand how SmartLINK has changed, the nature of the changes (e.g., improving functionality or increasing data collection), if its behavior has aligned with its mandate (e.g., as outlined in its contract) and its privacy policies. **We propose conducting a**

1. In this context, "participant provided" means that the people monitored are using their own smartphones, rather than a BI-provided phone with limited functionality.

retrospective analysis of this app and publicly-available documents [14] describing its data practices (e.g., privacy policies, contracts). We have collected 34 versions (APKs) of BI SmartLINK's Android app from May 2021 to January 2026 from online APK repositories (i.e., APKPure). In addition to establishing a ground truth regarding the evolution of SmartLINK for immigration surveillance and ensuring compliance with its contractual and regulatory obligations, our findings may also enable us to identify opportunities for future audits of technologies provided by government contractors. There is potential for these methods to be expanded to other apps in the immigration context, such as CBP One. Understanding the nature of the changes to the code and capabilities of SmartLINK can inform regulators about the type of modifications they may need to be wary of in the future when dealing with similar government technologies developed by external actors.

2. Related Work

Lerner et al. conducted a retrospective analysis of online web tracking from 1996 to 2016 [15]. They leveraged the Internet Archive's Wayback Machine to analyze tracking behaviors on archived webpages. In addition to presenting the findings of their measurement study, they devoted significant space to discussing the limitations of using the Wayback Machine for this type of analysis. In our work, we will use the Wayback Machine to analyze public websites and how they changed (or not) as the app's code has changed.

In work on the geographic variations of the same app in mobile app stores across the world (and their security and privacy implications), Guo et al. developed FREELENS—a framework that leverages API-bounded, call-path profiling and LLMs to study code-level differences between the same app from different marketplaces (e.g., Germany and India) [16]. We plan to use parts of this framework to understand code-level differences between updates of the app and what the security and privacy implications of these updates might be.

3. Open Questions

1) Which specific (technical) attributes of SmartLINK should we analyze over the time? The possibilities include permissions, third-party libraries, call paths, features, how these features are implemented in the code, etc.
2) What specific documents should we analyze over the time? The possibilities include privacy policies, public contracts, press releases, etc.
3) How can this work (and/or its framing) be improved to have a stronger impact?

References

[1] P. Mozur, A. Satariano, and A. Krolik, "This Company's Surveillance Tech Makes Immigrants 'Easy Pickings' for Trump." [Online]. Available: https://www.nytimes.com/2025/04/14/technology/trump-immigration-tech-geo-group.html

[2] Aly Panjwani and Julie Mao, "ICE Digital Prisons: The Expansion of Mass Surveillance as ICE's Alternative to Detention." [Online]. Available: https://web.archive.org/web/20240415162858/https://www.flipsnack.com/justfutures/ice-digital-prisons-1u8w3fnd1j/full-view.html

[3] E. Trovall. The growing business of immigrant surveillance. Marketplace. [Online]. Available: https://www.marketplace.org/2023/08/02/the-growing-business-of-immigrant-surveillance/

[4] T. Hanson, L. Geller, J. Peña, J. Kelly, A. Munoz, and J. Sanchez. ICE's SmartLINK app tracks migrants by the thousands. Does it work? CBS News. [Online]. Available: https://www.cbsnews.com/news/does-ices-smartlink-app-work/

[5] G. M. N. del Rio. Meet SmartLINK, the App Tracking Nearly a Quarter Million Immigrants – The Markup. [Online]. Available: https://themarkup.org/the-breakdown/2022/06/27/meet-smartlink-the-app-tracking-nearly-a-quarter-million-immigrants

[6] TRAC. Comprehensive, independent, and nonpartisan information about immigration enforcement - alternatives to detention (ATD). Transactional Records Access Clearinghouse. [Online]. Available: https://tracreports.org/immigration/detentionstats/atd_pop_table.html

[7] S. Shah. Trump Has Made ICE the Largest Law Enforcement Agency in the Country. Truthout. [Online]. Available: https://truthout.org/articles/trump-has-made-ice-the-largest-law-enforcement-agency-in-the-country/

[8] Pablo E. Paez. The GEO Group Awarded Contract by U.S. Immigration and Customs Enforcement for Provision of Skip Tracing Services. The GEO Group, Inc. [Online]. Available: https://investors.geogroup.com/news-releases/news-release-details/geo-group-awarded-contract-us-immigration-and-customs-1

[9] ICE Extends Crucial Contract with BI Incorporated, Boosting GEO Group's Stock and Strengthening Immigration Monitoring Efforts. The Finance Herald. [Online]. Available: https://thefinanceherald.com/ice-extends-crucial-contract-with-bi-incorporated-boosting-geo-groups-stock-and-strengthening-immigration-monitoring-efforts/

[10] K. Owens, Y. Eiger, B. Radka, T. Kohno, and F. Roesner, "Understanding experiences with compulsory immigration surveillance in the U.S." in *Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency*, ser. FAccT '25. Association for Computing Machinery, pp. 887–899. [Online]. Available: https://dl.acm.org/doi/10.1145/3715275.3732057

[11] Aly Panjwani and Hannah Lucal, "Tracked & Trapped: Experiences from ICE Digital Prisons." [Online]. Available: https://notechforice.com/wp-content/uploads/2022/05/TrackedTrapped_final.pdf

[12] K. Owens, A. Alem, F. Roesner, and T. Kohno, "Electronic monitoring smartphone apps: An analysis of risks from technical, Human-Centered, and legal perspectives," in *31st USENIX Security Symposium (USENIX Security 22)*. Boston, MA: USENIX Association, Aug. 2022. [Online]. Available: https://www.usenix.org/conference/usenixsecurity22/presentation/owens

[13] U.S. Immigration and Customs Enforcement. Alternatives to Detention Frequently Asked Questions. ICE.gov. [Online]. Available: https://web.archive.org/web/20251002120827/https://www.ice.gov/atd-faq

[14] Just Futures Law, Mijente Support Committee, and Community Justice Exchange. Fact Sheet on ICE FOIA Lawsuit: ICE Documents Reveal Alarming Scale of Surveillance in ISAP program. [Online]. Available: https://static1.squarespace.com/static/62c3198c117dd661bd99eb3a/t/6512da273ccb7321c334ab6c/1695734312687/ATDFOIAFinal.pdf

[15] A. Lerner, A. K. Simpson, T. Kohno, and F. Roesner, "Internet Jones and the Raiders of the Lost Trackers: An Archaeological Study of Web Tracking from 1996 to 2016," in *25th USENIX Security Symposium*.

[16] J. Guo, Y. Nong, Z. Lin, and H. Cai, "Code speaks louder: Exploring security and privacy relevant regional variations in mobile applications," in *2025 IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society, pp. 4284–4302. [Online]. Available: https://doi.ieeecomputersociety.org/10.1109/SP61157.2025.00225