OCTOBER 20, 2025

Kilpatrick's Privacy Dispatch – October 20, 2025

by Meghan K. Farmer , Tatum Andres , Katherine S. Kubik

Here are some recent privacy and cybersecurity related news stories that caught our attention over the past couple of weeks.

Otter.ai Suit Highlights Risks of Using User Data to Train AI

Otter.ai is facing a federal class action in California alleging that its AI transcription tool, Otter Notetaker, secretly recorded private conversations on popular video conferencing platforms without proper consent. The tool provides real-time transcriptions for accountholders, but according to the complaint, it only seeks permission from the meeting host and even then, only if the host is not an Otter.ai user. Other participants cannot disable the tool, and if the host is an Otter.ai accountholder with an integrated account, the Notetaker can join meetings without any affirmative consent from attendees. The lawsuit further claims Otter used these recordings to train its speech recognition models, in violation of federal wiretap law and California privacy statutes.

The bottom line:
This case underscores the legal risks of using AI transcription tools and training AI on user data without clear, informed consent. Otter.ai's privacy policy claims it trains on "de-identified" recordings, but courts and regulators have been skeptical of such assurances. For example, a federal court in Illinois allowed BIPA claims to proceed where facial templates were created from images even without names attached, holding that the templates could still qualify as biometric identifiers. Regulators have also challenged anonymization claims when data could reasonably be re-linked to individuals, as seen in the FTC's 2021 settlement with Everalbum over facial recognition practices. As AI models increasingly rely on biometric, geolocation, and consumer behavior data, companies should expect heightened scrutiny.

What you need to do:
Companies developing or deploying AI-powered tools should carefully review how meeting data is collected and disclosed in privacy policies. Ensure consent is obtained from all participants, not just account holders. With respect to establishing use rights in data for AI training, avoid relying solely on de-identification. Updating product settings to provide notice and meaningful control can help reduce exposure to claims like those facing Otter.ai.

DOJ Guidance and Early Lawsuits Highlight Risks Under the Bulk Data Transfer Rule

On April 11, 2025, the Department of Justice (DOJ) issued guidance on the "Data Security Program" (Bulk Data Transfer Rule), which implements Executive Order 14117 restricting bulk transfers of U.S. sensitive personal data and government-related data to countries of concern, including China (including Hong Kong and Macau), Russia, Iran, and others. The Rule took effect on April 8, 2025, and carries both civil and criminal penalties.

Earlier this month, two federal class actions were filed against digital advertising platforms alleging violations of the Electronic Communications Privacy Act (ECPA) based on purported breaches of the DOJ's Bulk Data Transfer Rule. The complaints claim that the companies used tracking technologies on third-party websites to capture users' interactions and transmitted that data to a Chinese company (Temu), citing the DOJ Rule to strengthen their ECPA claims. Although the DOJ Rule does not provide a private right of action, these lawsuits appear to be the first efforts to leverage it as a foundation for civil litigation.

Under the ECPA, the "party exception" generally permits a party to a communication to intercept it. However, the exception does not apply if the interception is carried out knowingly and intentionally for the purpose of committing a criminal or tortious act—here, the alleged unlawful transmission of bulk U.S. sensitive personal data to a covered foreign entity in violation of the Bulk Data Transfer Rule.

Implications:
Adtech and other data-driven companies face heightened compliance risks. Even anonymized identifiers like IP addresses, cookies, and advertising IDs may qualify as "sensitive data." Plaintiffs and regulators alike are likely to scrutinize adtech data flows, particularly when foreign entities are involved.

What You Should Do:
Businesses should immediately:

- Map data flows involving advertising technologies, pixels, and trackers.
- Confirm that sensitive data is not disclosed to "covered persons," such as entities incorporated in China or other listed countries.
- Update contracts and diligence procedures for third-party partners, ensuring onboarding includes DOJ Rule compliance checks.

California Privacy Protection Agency (CPPA) Shows its Teeth in Tractor Supply Settlement

Last month, the CPPA reached a settlement with Tractor Supply Company, requiring Tractor Supply to pay a $1,350,000 fine for violations of the California Consumer Privacy Act (CCPA). This represents the CPPA's largest settlement so far, the enforcement action most focused on personal information used in an employment context, and, according to the head of enforcement of the CPPA, reflects the CPPA's "priority to investigate whether businesses are properly implementing privacy rights".

Tractor Supply ran afoul of the CCPA in four ways: (1) failing to maintain a privacy policy that notified consumers of their rights; (2) failing to notify California job applicants of their privacy rights and how to exercise them; (3) failing to provide consumers with an effective mechanism to opt-out of the selling and sharing of their personal information; and (4) disclosing personal information to other companies without entering into contracts that contain privacy protections. In addition to remediating these failings, Tractor

Supply must also run quarterly scans of its digital properties to maintain a complete inventory of its tracking technologies, implement a program to monitor its processing of opt-out signals, conduct annual reviews of how personal information is collected through tracking technologies, and provide written certifications of compliance to the CCPA for a period of five years.

The settlement highlights the need for continued review and monitoring of your privacy program to ensure its continued compliance with privacy laws and that your privacy program accurately reflects how your business collects and uses personal information. It is also important to give effect to the consumer rights described in your privacy policy and to respect the opt-out signals and requests submitted by consumers. Finally, this settlement serves as an important reminder that the CCPA provides privacy rights to your employees, not just consumers. California is one of the only states to do so and it is important not to overlook your California employee's (including job applicants', contactors', and former employees') privacy rights when putting together your privacy program.

Be sure to follow the firm's LinkedIn page to see more of these news snippets with our commentary.