whizardries

Lex Protego, PLLC

Email Pixel Tracking Litigation

What Happened & Implications

Prepared For:
ESPC General Meeting

Visit Our Website
www.lexprotego.com
www.whizardries.com

Making the Arcane Simple

HP & Pretexting: A brief history

Background and Discovery

- In 2006, HP hired private investigators because board members were leaking things to the press.
- Investigators used "pretexting" to access phone records.
- They also used ReadNotify's product to try to get information about email forwards.

Legislative Response

- The U.S. Congress passed the Telephone Records and Privacy Protection Act of 2006, making fraudulent access to phone records illegal.
- Arizona passed the Telephone, Utility, and Communication Service Records Act (TUCSRA)

Arizona TUCSRA Summary

- **Prohibits unauthorized access**: The Act makes it illegal to obtain, sell, or transfer personal communication records without authorization.
- **Protects customer data**: It requires companies to implement reasonable security measures to safeguard customer information.
- **Applies to various records**: The Act covers telephone records, communication service records, and public utility records.
- **Penalties for violations**: Violators may face civil and criminal penalties, including fines and imprisonment.
- **Provides private right of action**: Individuals can sue for violations of the Act, potentially recovering damages and attorney's fees.

What's pretexting got to do with it?

27. Six days after the hearing, the California Attorney General indicted Dunn, Hunsaker, DeLia, and two private investigators involved in both iterations of Project Kona.[49] A few months after that, Congress passed the Telephone Records and Privacy Protection Act of 2006, a law that criminalizes "knowingly and intentionally obtain[ing], or attempt[ing] to obtain, confidential phone records information of a covered entity, by making false or fraudulent statements or representations to an employee of a covered entity." 18 U.S.C. § 1039(a)(1). That law, as the text suggests, only prohibits pretexting, not the use of email trackers.

28. After Congress enacted the TRPA, the Arizona legislature went a step further, passing a law that addressed *both* methods used by HP's investigators. Like the federal law, this new Arizona law prohibits any person from procuring or conspiring with another to procure "a telephone record" of residents without consent. But, in addition, the new law also prohibits procurement of any "communication service record" (including email records) of "any resident of this state without the authorization of the customer to whom the record pertains, or by fraudulent, deceptive, or false means." Ariz. Rev. Stat. Ann. § 44-1376.01. And while Congress declined to include a private right of action in the federal law, the Arizona legislature allowed residents to pursue civil remedies. Ariz. Rev. Stat. Ann. § 44-1376.04(2).

B. Email Pixels

29. Despite Arizona law prohibiting the practice, companies still embed trackers within emails without first obtaining consumers' consent. Indeed, "[a] 2018 Princeton study on email tracking tested over 12,000 emails from 900 senders offering mailing list subscriptions and found that 70% contained trackers."[50]

30. These trackers, known as "spy pixels," enable companies to learn information about the email transfer, including when and where the email was opened. Pixel are used to log when the recipient accesses the email and can record the number of times an email is opened, the IP address linked to a user's location, and device usage.[51]

31. The use of spy pixels is a "grotesque invasion of privacy" according to industry advocates.[52]

32. To activate a spy pixel, recipients only need to open the email. The recipient does not need to directly engage with the pixel—when an email is opened the tracking pixel is automatically downloaded.[53]

33. A spy pixel is typically a 1x1 (one pixel high by one pixel long) image. "The spy pixel is so small it is basically impossible to see with the naked eye."[54]

Who got sued?

- Saks.com
- Nordstrom
- Urban Outfitters
- Home Depot
- TJX Companies
- Lowes
- Target
- Gap
- Patagonia
- Signet Jewelers
- Burlington Coat Factory
- Office Depot
- Validity
- Salesforce
- Infillion (f/k/a PaeDae)
- F&M Fashion

Lex Protego, PLLC

whizardries

Communication Service Record?

All of these cases allege that brands are improperly obtaining “communication service records”

"Communication service record" includes subscriber information, including name, billing or installation address, length of service, payment method, telephone number, electronic account identification and associated screen names, toll bills or access logs, records of the path of an electronic communication between the point of origin and the point of delivery and the nature of the communication service provided, such as caller identification, automatic number identification, voice mail, electronic mail, paging or other service features. Communication service records do not include the content of any stored oral, wire or electronic communication or a telephone record.

Urban Outfitters moves to dismiss

- Two grounds
  - Lack of standing
  - Lack of a valid legal claim (so what?)

What is standing?

- "What's it to you?" – A. Scalia
- "Do you have a dog in this hunt?" – Texas

1. Actual (or threatened) injury
2. Injury due to the defendant's action
3. A court ruling can do something to help

Point, © Carol Blyberg, CC BY-NC 2.0

The Argument

- Plaintiffs must show an injury of a type traditionally recognized
  - The closest are “intrusion upon seclusion” or “public disclosure of private facts”
  - Both require showing a violation that would be “highly offensive” to a reasonable person
- Part of what makes this inoffensive is that the plaintiffs asked for the messages
  - This distinguishes these cases from others alleging things like TCPA violations
- No one (in federal or state courts) has tried this expansion

The judge agrees

"As a matter of law, the Court concludes that digital records reflecting merely the dates and times at which Plaintiff opened promotional emails she signed up to receive, and the length of time she spent reading them, are not sufficiently personal to support a concrete injury. Like a users' keystrokes and mouse clicks upon voluntarily visiting a retailers' website, these details are entitled to less privacy protection by virtue of Plaintiff's decision to opt into receiving and reading the emails."

Memorandum Opinion, *Hartley v. Urban Outfitters, Inc.*, No. 2:23-cv-04891 (E.D. Penn. 07/17/2024), ECF No. 17, at 13.

Impact on other cases

- Voluntary dismissal
  - Dominguez
  - Smith
  - Knight
  - Torrez
  - Encinas
- Dismissal
  - F&M Fashion
- Motion to Dismiss
  - Mills
  - Campos
- Motion to Dismiss
  - Carbajal v. Home Depot
  - Segovia

What is an HTMLized email?

- Contains HTML that works just like a webpage
- A loss in a case like Hartley would have really hurt

- H&M's court made a stronger ruling that already being cited in the remaining cases:
  - "The Court concludes that the information at issue here—when and how an email was opened, how long it was opened, what device was used, the associated IP address of the recipient, and whether it was forwarded— is not a 'communication service record' or a type of 'access log' protected by TUSCRA (*sic*). The Court does not accept Plaintiff's expansive interpretation of the statute." *D'Hedouville v. H&M Fashion USA, Inc.*, No. C20243386 (Ariz. Super. Ct. Oct. 11, 2024)

Takeaways

1. The plaintiff's bar is trying to find ways to sue over privacy
2. Brands are at greatest risk, but service providers are not immune
3. No one understands how even old technology works
4. Consent is an excellent guardrail

whizardries

Lex Protego, PLLC

Thank you

936-657-4858

5506 Camaguey St, Houston, Tx 77023