

Digital Compliance: What's New (and Risky) in Privacy, Tech, and AI

Practical Guidance on Cutting-Edge Concerns

2023 New Legal Risks Symposium

SEPTEMBER 20, 2023

www.gtlaw.com

Agenda (Scary Scenarios)

1. Cookie Lawsuit
2. Data Retention
3. Generative AI
4. Website Scraping
5. Mobile App Removal
6. Digital Accessibility Claim
7. Data Subject Request Aggregator

About The Data

GT conducts a comprehensive survey of the privacy and compliance practices of the entire Fortune 500, as well as the 100 most downloaded mobile apps in each app store. Data in this presentation is pulled from this survey.

Scenario 1: Cookie Lawsuit

You receive a class action demand letter alleging that your website's use of the Meta pixel violates the federal Wiretap Act as well as a variety of state laws.

Plaintiff found the alleged violation through commonly available settings in their social media account, and through use of your site.

Plaintiff alleges \$15k in statutory damages for each occurrence, with potentially millions of occurrences across the class.

Cookie Lawsuit: Background

- Under the Federal Wiretap Act, a person is prohibited from “intentionally intercept[ing] ... any ... electronic communication.”
 - States have equivalent rules with varying consent standards
 - 2022 3rd and 9th Circuit decisions have increased litigation.
- Three technologies: Session replay, chatbots, and use of the Meta pixel.
- HIPAA and VPPA should also be considered.
- Compliance overlaps with, but is not the same as, new U.S. privacy laws.



Meta Pixel Helper

[Learn More](#)



One pixel found on [www.████████.com](#)



Meta Pixel

[Troubleshoot Pixel](#)

Pixel ID: 147821091243████████ [click to copy](#)

[Set Up Events](#) New!

▶ ⚡ Microdata Automatically Detected ⓘ

▼ ✅ PageView

EVENT INFO

Setup Method: Manual

URL called: [Hide](#)

`https://www.facebook.com/tr/?id=147821091243████████&ev=PageView&dl=https%3A%2F%2Fwww.████████.com%2Fterms%2F&rl=&if=false&ts=1686067252812&sw=1920&sh=1080&v=2.9.106&r=stable&ec=0&o=30&fbp=fb.1.168606725████████1920273075&it=1686067252698&co=false&rqm=GET`

Load Time: 128.13 ms

Pixel Code: [Hide](#)

`fbq("track", "PageView")`

Pixel Location: [Hide](#)

`https://www.████████.com/terms/`

Frame: Window

Cookie Lawsuit: What Now?

- These are nuisance claims, but uncertain enough to command higher values:
 - Settlement range: \$25k-\$100k, depending on a variety of factors
 - 7-figure settlements have happened
 - Possible reputational issues if the claim proceeds
- Expect new claims until remediation and mitigation of issues
- While claims are currently limited to select, more common pixels *the claim could apply to numerous technologies*

Cookie Lawsuit: What Now?

- Use experienced counsel: Most of these claims are coming from a handful of plaintiff's firms, meaning experience with opposing counsel is a key advantage.
- Leverage your terms of use: A well-drafted terms of use with a strong arbitration provision (with mass arbitration defense), class action waiver, and limitation of liability can drive down cost.
- Be aggressive: Typical plaintiff firms are looking for a quick win, so show expertise and show willingness to litigate.

Cookie Lawsuit: Prevention & Mitigation

- **Can you remove the technology?** Removal is the only way to guarantee no further claims.
- Upgrade your terms of use
 - Arbitration (with mass arbitration controls), class action waiver, limitation of liability, try for consent here as well
- Audit your cookie/adtech/pixel use
 - Not just on your homepage, not just your current geographic location
- Don't forget about your mobile app!

Cookie Lawsuit: What if We Can't Remove the Pixel?

- Implement a notice and consent structure
 - Prior, explicit, opt-in consent
 - Opt-out structures such as those required by new U.S. privacy laws arguably *do not reduce the risk of these claims*
 - Notice banner arguably not enough, as individual only receives notice *after* pixel is deployed
 - Mention third parties in your banner language
- Consider geofencing to avoid state law claims, high-risk circuits
- Disclose in your privacy policy



This website uses cookies to improve your experience. [Learn more](#)



Tracking technology, such as cookies, are important for the correct functioning of our websites. By clicking "Allow All" you are also directing us to use tracking technology and non-service provider cookies, and to share your information with third party advertising and analytics providers, some of whom may be based in the United States. You can configure your preferences by clicking on the "customize settings" link below.

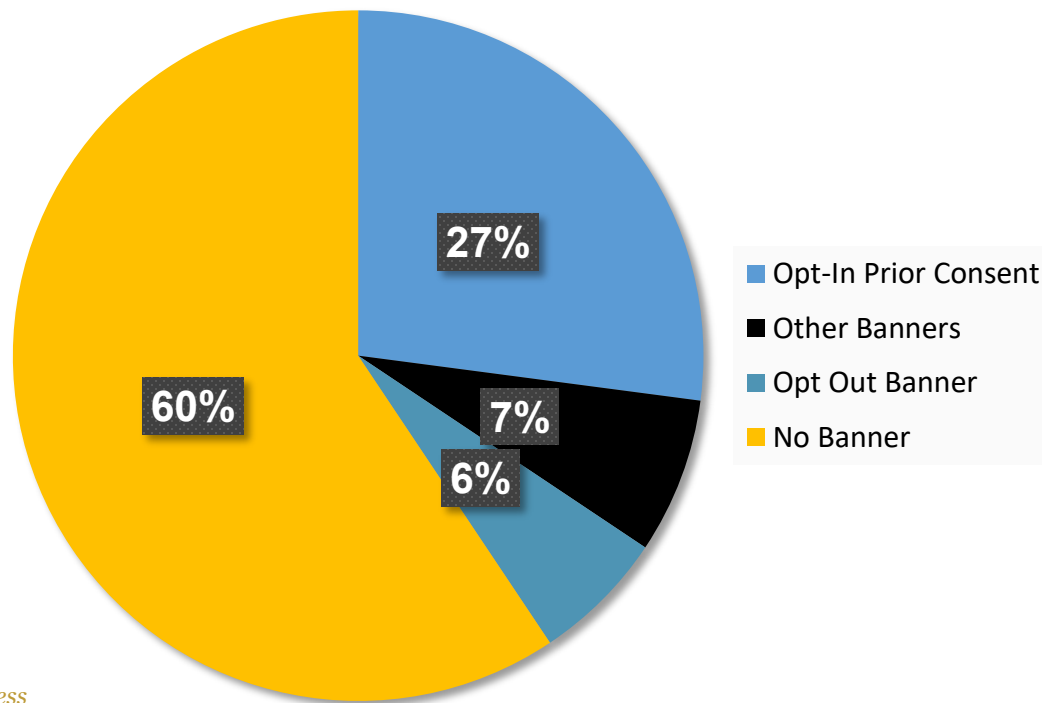
[Privacy Notice.](#)

[Customize Settings](#)

[Allow All](#)

[Decline Optional](#)

Fortune 500 Cookie Consent Banners



As seen from a California IP Address

Scenario 2: Personal Information Retention

Your company is attempting to implement data minimization as required by new privacy laws such as the Colorado Privacy Act. Personal Information is stored in dozens of company systems. Business leaders are insisting information must be kept indefinitely, either for regulatory requirements or marketing efforts.

While pondering this at the water cooler, Toby in HR mentioned 5 filing cabinets filled with customer records in the annex.

Personal Information Retention

- “Personal Data should only be kept in a form which allows identification of Consumers for as long as is necessary for the express Processing purpose(s). To ensure that the Personal Data are not kept longer than necessary, adequate, or relevant, Controllers shall set specific time limits for erasure or to conduct a periodic review.”
 - [4 Colo. Code Regs. § 904-3:6.07](#)

Personal Information Retention

- **Implement a retention policy AND schedule**

- These need to be realistic: don't over-promise, use an implementation delay if needed.

- **Policy**

- Include the Who, What, Where, Why, and How of deletion
- Who is responsible? Business units? Legal?
- Integrate legal holds

- **Schedule**

- Definitive period start dates
- Minimum periods as required by applicable laws
- Maximum retention periods as required by privacy law
 - Indefinite retention isn't reality
- Include physical documents
- Include citations to applicable laws

LEGEND

The following abbreviations are used to help define the applicable Retention Period beginning date for each category of records:

C	For Contractual Matters, the Latest End Date whether due to Purchase, Sale, Full Performance, Payment, Breach, Termination or Final Resolution of Dispute;	J/S	For Litigation or Arbitration Related Matters, the Latest Date of When a Dispute Ended, such as Final Judgment Entered, Settlement Made or Payment or Performance Completed;
CR	Latest of Creation of Record, Most Recent Editing of Record or Filing of a Return or Report to which Record is Relevant. In the case of Tax Records, CR begins after the due date of such tax for the return period to which the record relates, or the date such tax is paid, whichever is the later;	PROP	Latest of When Property or Interest Sold or Disposed of or Final Resolution of Dispute;
E	For Employment Related Records, the Latest Date of When Separated, Retired or Terminated from Employment, When Employment Application Rejected, When Job Posted, or Final Resolution of Dispute;	S/O	Superseded/Obsolete. When a Record has been Superseded by another Record, or is Otherwise Obsolete with no Further Legitimate Business Purpose or Use to the Company;
		TRM	Latest of Term or Period of Coverage or Applicability; Life of Benefit; or Period within which a Claim Must be Made.

ASSETS	Tangible Capital Assets and Property	Real estate and fixtures; tangible capital property with a useful life longer than one year	Latest of PROP + 6 years, C + 3 years or S/O + 3 years	Consideration of applicable statutes of limitation for suits on contracts and a business judgment regarding the average delay in bringing suit after a breach of contract See also 26 U.S. Code § 6501 (6 years after return filed, under Internal Revenue Code)
--------	--------------------------------------	---	--	---

Scenario 3: Generative AI

Other departments are pressuring legal to approve the use of generative AI, including LLMs, for company tasks including communications, marketing, coding, and editing.

Simultaneously, employees are using their personal ChatGPT accounts for work functions. The extent to which this is happening is unknown.

You are receiving pressure both to allow the use of these technologies and to ban them.

Generative AI: Recommendations

- Implement an AI use policy
 - Be realistic: Outright prohibition is unlikely. Instead, focus on controlling specific inputs or activities.
 - Example: Prohibit input of personal information, code
 - Include approval and escalation processes: Rather than prohibition, an approval and escalation process for higher-risk uses can prevent circumvention of the policy.
 - Whitelists: Create an approved list of technologies, use cases, or both.
 - Eliminates uncertainty and encourages use, saves approval process bandwidth
- Understand platform terms

Generative AI: Recommendations

- Don't Forget Customer Contracts!
 - Will use of AI violate confidentiality obligations?
 - Can AI systems satisfy security requirements?
 - Would a customer be surprised to find out you're using generative AI?
- Use business accounts and logins, if available

Scenario 4: Website Scraping

Your company is scraping massive amounts of publicly available data from the internet, including LinkedIn profiles.

At the same time, you believe your biggest competitor is scraping large amounts of data off your platform. Your CEO has asked you to stop them and bring a claim against them.

You're also worried that AI platforms are scraping your data for their purposes.

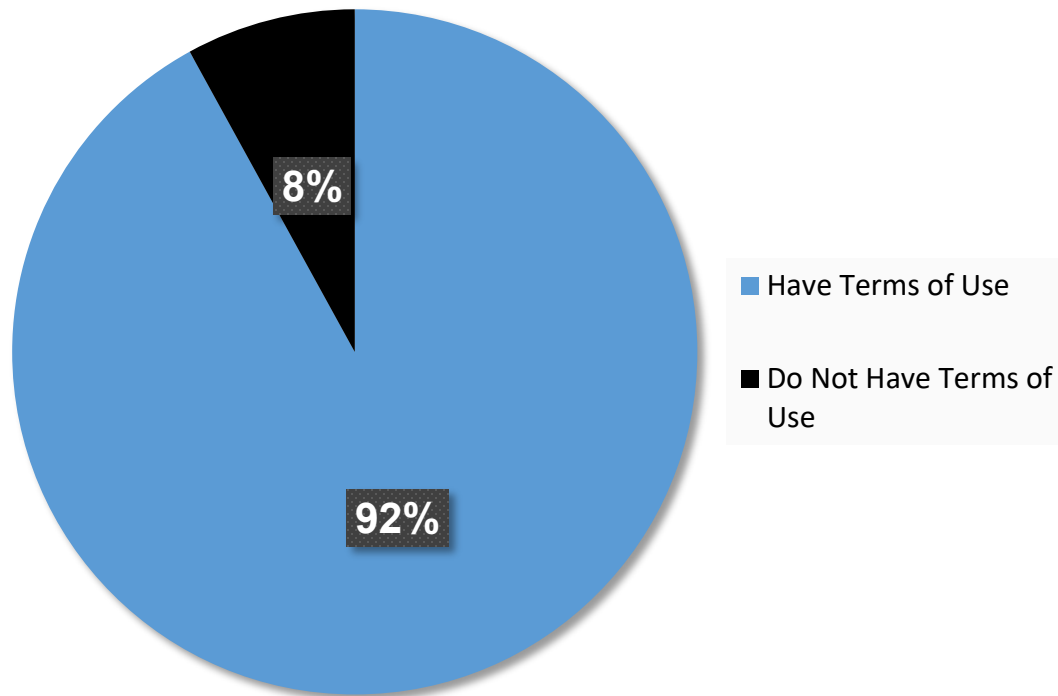
Website Scraping: Legality

- Scraping is *generally* completely legal absent specific controls.
 - The Computer Fraud and Abuse Act (CFAA) can protect data behind password walls, accounts.
 - The Digital Millennium Copyright Act (DMCA) can create liability for IP related scraping.
 - State and case law is generally permissive, but a variety of low strength common law claims exist.
 - Trespass to chattels, unjust enrichment
- There are material privacy issues if scraping personal information

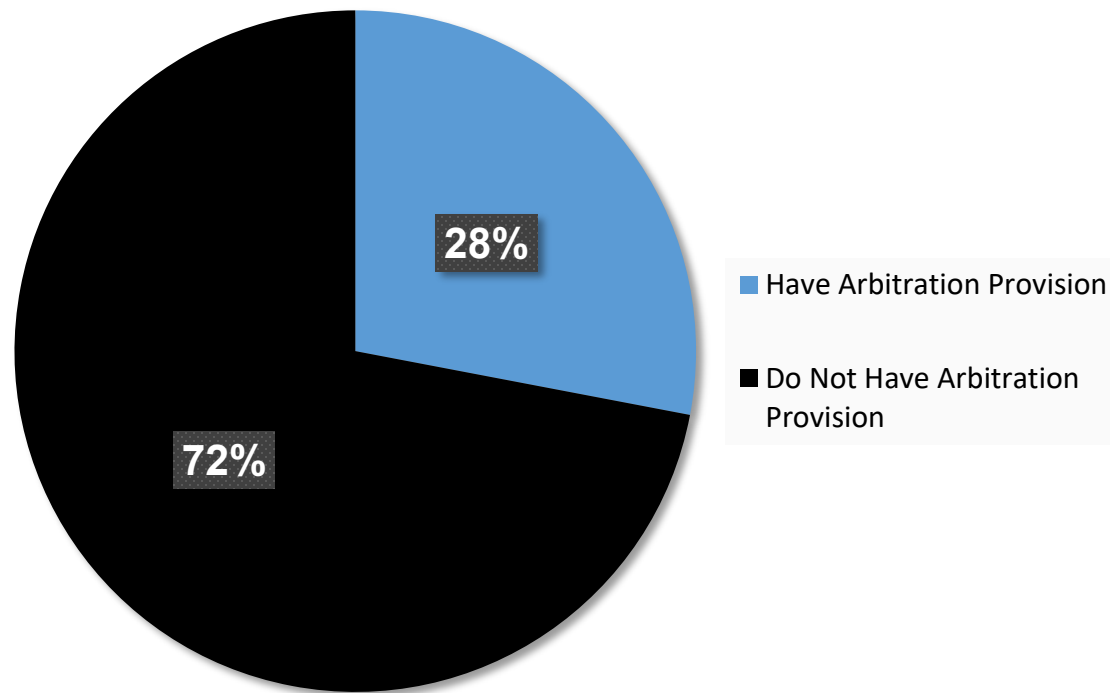
Website Scraping: Defenses

- Legal measures
 - Terms of use: Prohibit scraping, ensure enforceability
 - Account creation: Arguably triggers CFAA, makes terms more enforceable, provides technical barrier
- Technical measures
 - CAPTCHAs and similar technologies
 - Robots.txt file
 - Detection and authentication

Fortune 500 Websites



Fortune 500 Terms of Use Arbitration



Scenario 5: Mobile App Removal

You receive a notice from an app store that your Company's app doesn't comply with some of the hundreds of app store requirements, including providing an accurate privacy nutrition label and the ability for all users to delete their accounts. The store has warned that the company has 5 days to fix these issues, or your app will be removed from the app store.

On the same day, you also receive notice from the CA AG that the use of tracking technologies in your app could trigger investigation.

Mobile App

- App stores have hundreds of requirements, violating any of which could lead to an app being removed or not approved.
- Recommendations:
 1. Audit your app for all app store requirements
 2. Ensure privacy nutrition label accuracy and cohesion with privacy policy
 3. Consider independent security verification for Google Play store
 4. Post a comprehensive terms of use, do *not* rely on the default terms
 5. A broad, easy-to-use deletion mechanism is a must

Data Collection

Next, select all of the data that **you or your third-party partners collect from this app**. If your app is currently available on the App Store, make sure your responses reflect the data collected **only from that app version**.

Data types that meet **all of the following criteria are optional to disclose**:

- The data is **not used for tracking purposes** (meaning the data is not linked with other third-party data about the user or device for advertising or advertising measurement, or shared with a data broker). For more detail, see [App privacy details on the App Store](#).
- The **data is not used for Third-Party Advertising**, your Advertising or Marketing purposes, or for Other Purposes, as those terms are defined in [App privacy details on the App Store](#).
- Collection of the **data occurs only in infrequent cases** that are **not part of your app's primary functionality**, and which are optional for the user.
- As part of the interface in your app where the user provides the data to be collected, such **data must be transparent to the user at the time of collection**, the user's name or account name must be prominently displayed in the submission form alongside the other data elements being submitted, and the user must affirmatively choose each time to provide the data for collection.

If the data type collected by your app meets some, but not all, of the above criteria, it must be disclosed in your privacy section.

Contact Info

- ☒ **Name**
Including first or last name
- ☒ **Email Address**

[Back](#)

[Cancel](#)

[Save](#)

"Pal About" would like permission to track you across apps and websites owned by other companies.

Your data will be used to deliver personalized ads to you.

[Allow Tracking](#)

[Ask App Not to Track](#)



Data Used to Track You

The following data may be used to track you across apps and websites owned by other companies:

- | | |
|----------------|------------------|
| Purchases | Financial Info |
| Location | Contact Info |
| Search History | Browsing History |
| Identifiers | Usage Data |

Data safety →

Safety starts with understanding how developers collect your use, region, and age. The developer provided this inf



No data shared with third parties
[Learn more](#) about how developers declare sharing



This app may collect these data types
Location, Personal info and 7 others



Data is encrypted in transit



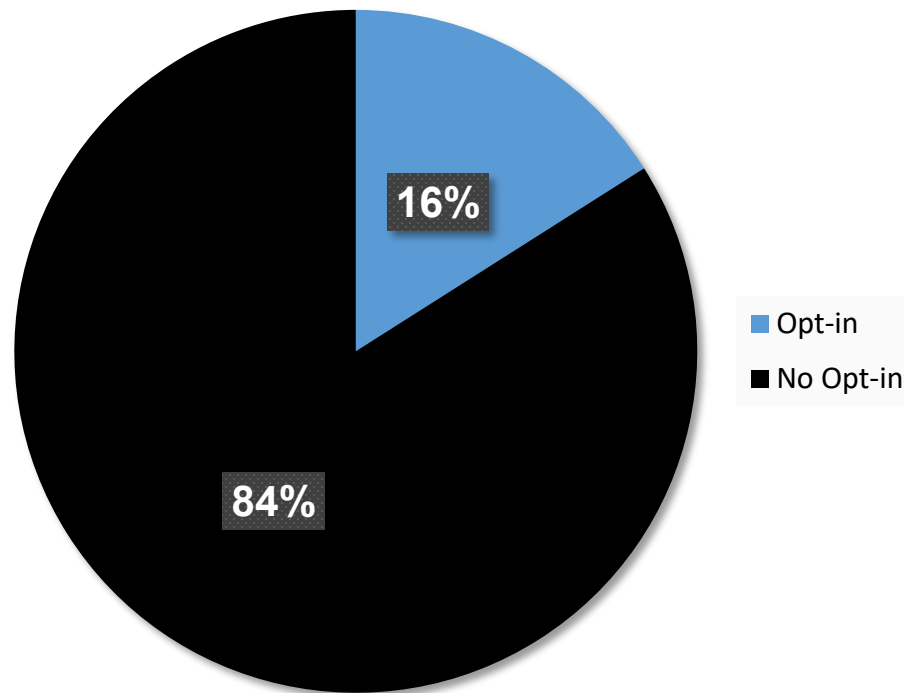
You can request that data be deleted



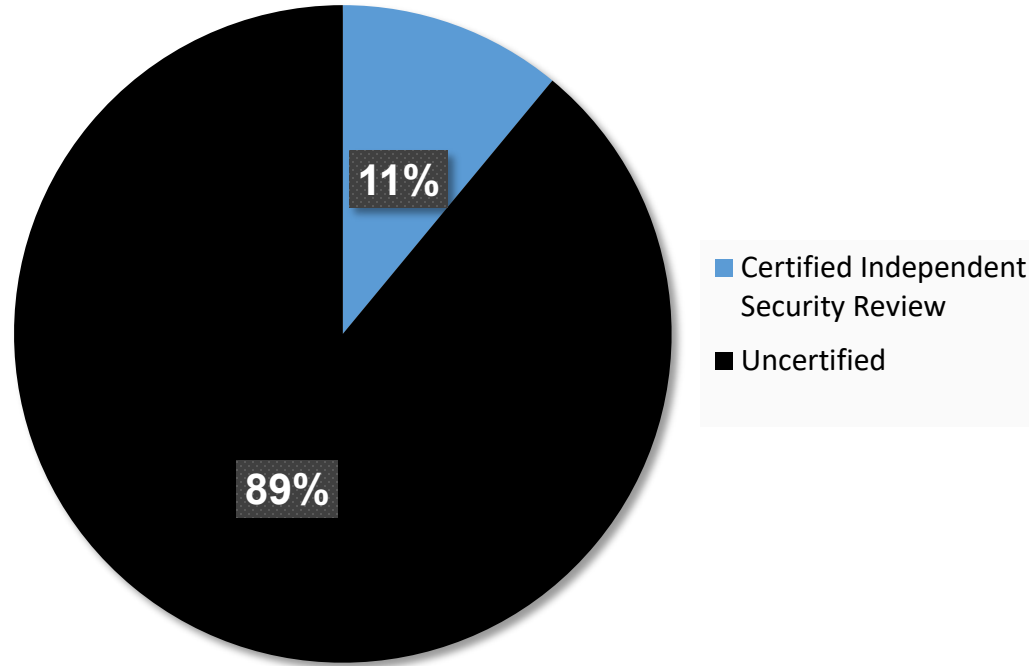
Independent security review

[See details](#)

Top 100 Mobile Apps: Apple Sharing Opt-In



Top 100 Mobile Apps: Independent Security Review



Scenario 6: Digital Accessibility Claim

You receive a demand letter alleging that your website is inaccessible to users who need assistive technology.

You're surprised because your company pays for an accessibility overlay widget which adds controls to your site that the overlay provider says makes it fully compliant.

Plaintiff's counsel is asking for \$50k to settle. The overlay widget provider isn't responding to your emails, and their contract says they will only indemnify you from damages resulting from a final judgment.

Digital Accessibility Claim: What Now?

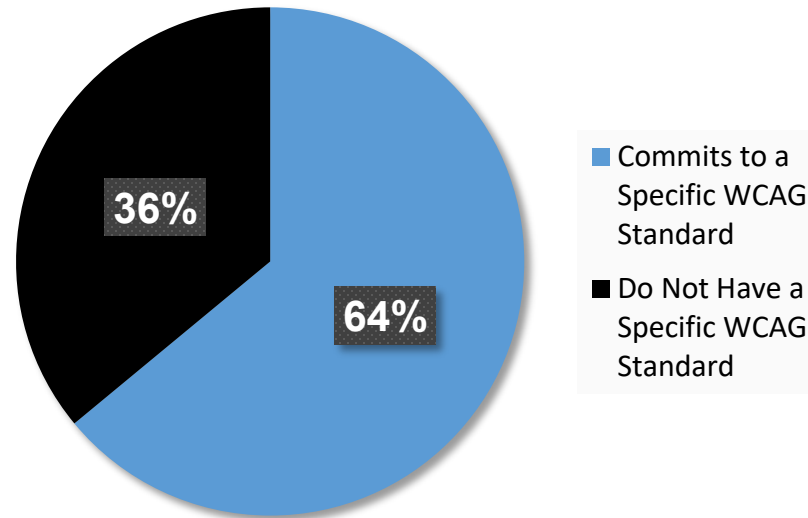
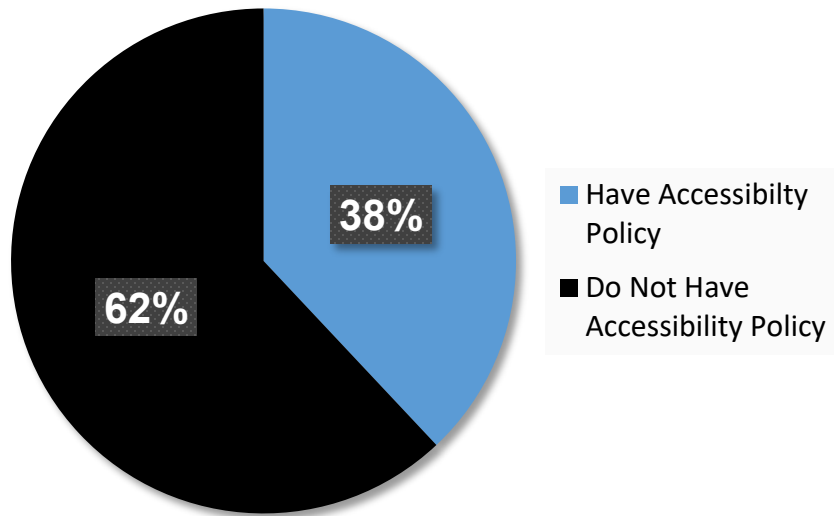
- Another nuisance suit, with typical settlement values from \$15k-\$60k
- Typical settlement includes not only compensation, but also commitments to:
 - Remove overlay widget
 - Comply with the Web Content Accessibility Guidelines (WCAG)
 - Institute external and internal accessibility policies, training
 - Conduct professional monitoring

Digital Accessibility Claim: Prevention and Mitigation

- Remove Overlays: Data suggests overlay widgets *increase* your likelihood of suit.
 - They also are under attack by accessibility advocates for making websites less accessible.
- Comply with WCAG 2.1 AA
 - This standard is also required by state privacy laws.
- Add accessibility policies, both internal and external.
- Improve your terms of use.



Fortune 500 Accessibility Policies



Scenario 7: Data Subject Request Aggregator

To date, you have received 1-3 data subject requests per month to the privacy email inbox you set up. Budget is tight, so you've been handling these yourself. You return from a long weekend to find 103 new requests, all with the same formatting and language. Some requestors don't even appear in your systems.

You are unsure how you'll respond to all the requests in time...

Data Request Aggregator: Background

- Request aggregators send out mass amounts of requests on behalf of individuals.
 - These are typically deletion requests.
 - Can be identified by formulaic and identical language. Sometimes the aggregator will identify itself and be readily apparent.
- Requests are typically sent to every company on the aggregators “list,” regardless of whether that company actually has the requestor’s data.

Data Request Aggregator: What Now?

- Determine if its possible to honor the requests.
 - Narrow down the universe:
 - How many requestors do you actually have data on?
 - How many are in states that grant them rights?
 - Can the aggregator be considered an authorized agent?
- If you need to deny:
 - Not a valid authorized agent
 - Against company policy to respond to aggregators due to lack of verification

Data Request Aggregator: Mitigation

- Control the intake point
 - Use a webform with a CAPTCHA
 - If using email, don't use a common address
 - i.e. Privacy@Company.com
 - Require notarization and provide reimbursement
- Increase request response automation
- Try to remove yourself from aggregator platforms
 - Cease and desist, breach of terms of use

More Information



Tyler Thompson

Denver

[303.685.7437](tel:303.685.7437)

ThompsonTy@gtlaw.com

www.linkedin.com/in/tylerjthompson

GT's Data Privacy Dish

- <https://www.gtlaw-dataprivacydish.com/>

GT's Emerging Technology Blog

- <https://www.gtlaw-emergingtechnologyviews.com/>