October 25, 2024

Small Missteps, Big Consequences: Lessons for Privacy Programs from Recent Enforcement Actions

Matt Dumiak
CompliancePoint

Shaundra Watson
BSA

Aaron Burstein
Kelley Drye & Warren

Privacy+ Security Forum

Speakers

Privacy+ Security Forum

Aaron Burstein

Partner
Kelley Drye & Warren

Shaundra Watson

Senior Director, Policy
BSA

Matt Dumiak

Director, Privacy Services
CompliancePoint

Agenda

How do investigations get started?

Cookie banners

Responses to consumer privacy requests

Privacy policies and user interfaces

Privacy+ Security Forum

An Origin Story: How does an investigation start?

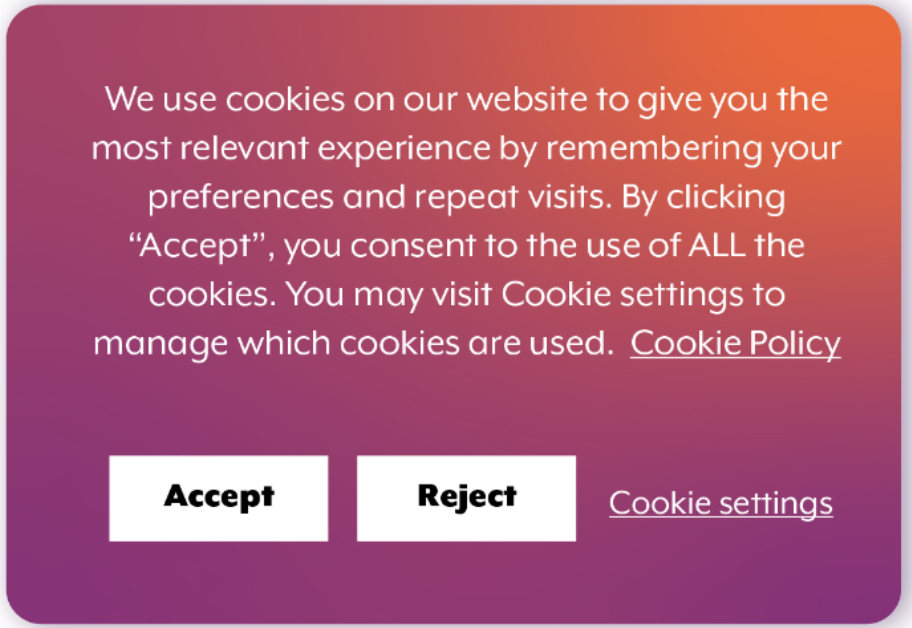
Privacy+ Security Forum

Cookie Banners

Privacy+ Security Forum

What’s behind all the banners?

NY AG Guidance (July 2024)



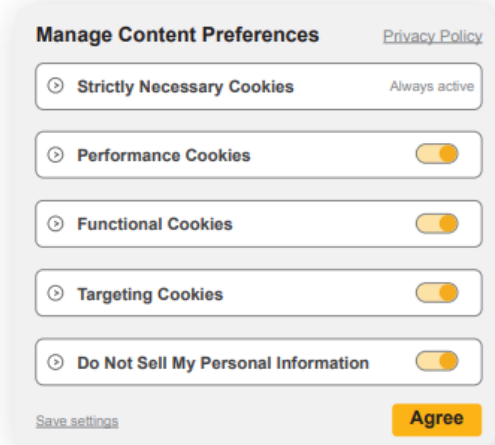
Cookie pop-up

Unfortunately, not all businesses have taken appropriate steps to ensure that their disclosures are accurate and that privacy controls work as described. An investigation by the Office of the New York State Attorney General (OAG) identified more than a dozen popular websites, together serving tens of millions of visitors each month, with privacy controls that were effectively broken. Visitors to these websites who attempted to disable tracking technologies would nevertheless continue to be tracked. The OAG also encountered websites with privacy controls and disclosures that were confusing and even potentially misleading.

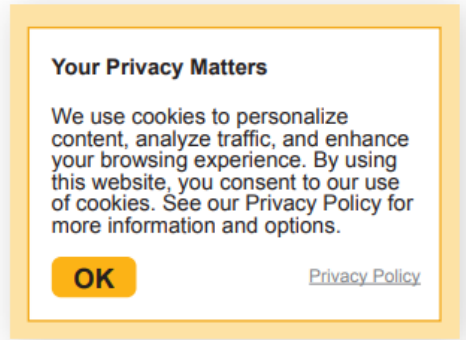
CPPA Guidance (Sept. 2024)

Business A is considering user interface designs to seek consumers' consent to use their personal information and to honor requests to opt out of sale. Business A is reviewing versions designed by a service provider as well as ones designed in house.

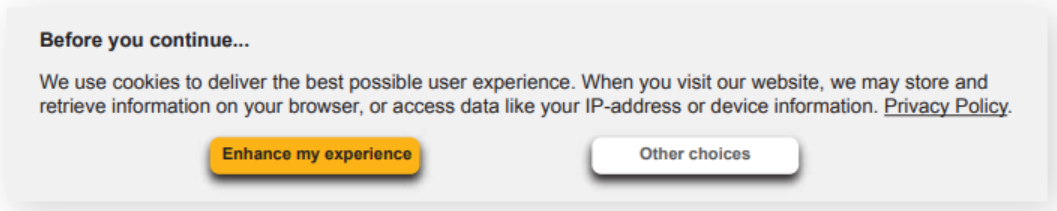
SAMPLE ONE



SAMPLE TWO



SAMPLE THREE



Cookie Banners: Tips and Action Items

- Understand Your Data
  - Regulators are focused on sensitive data: health, children, etc.
- Compliance Testing
  - Updated privacy notices and banners aren’t cutting it anymore
- Website Governance
  - Banner language, placement, choices
  - Cookie/tag categorizations
  - Process for adding/removing cookies
- Watchful Eye on Litigation and Enforcement Trends
  - Seek out resources to stay updated

Privacy Policy Pitfalls

Privacy+ Security Forum

What you say can be used against you

Privacy+ Security Forum

What kinds of statements garner scrutiny?

- Providing “California Privacy Rights” (but not including other states)
- Tentative, open-ended statement about collection, use, disclosure purposes
  - E.g., “We may collect data for any of the following purposes . . .”
- Using “anonymous” or “deidentified” information for advertising
- We use automated tools to improve our services.

Does Use of AI Affect What You Say in Your Privacy Policy?

Privacy+ Security Forum

- **The AI Effect: Key Questions That Could Affect Your Privacy Disclosures**

  - **Sharing data.** Are you sharing data with additional companies, e.g., a third-party generative AI provider whose AI model is integrated in your service provider's software? Is the third-party gen AI provider retaining the data or using it to train its AI model? Is this data sharing captured by the existing privacy policy language?

  - **New uses.** Does use of AI enable the business to leverage the personal data for additional purposes and, if so, are these purposes adequately described in your policy? Do any of these purposes include profiling or making significant decisions, which trigger additional obligations? Does your policy address the use of data to train AI systems for product improvement and how it is used for that purpose?

  - **New disclosures.** Do you know what you are doing with AI, such as enhancing a gen AI system's performance with your own company's data? If so, are you prepared to comply with new laws requiring disclosures on websites on all data used to train generative AI systems?

Tips

- Avoid vague and overbroad statements.
- Adequately describe consumer rights and how to exercise them.
- Prioritize clarity.
  - Regulators have flagged instances where explanations of opt-outs were confusing.
- Consider implications of AI.
  - Make sure you ask the right questions to know whether your data sharing and use align with your privacy policy.
  - Prepare for new laws and forthcoming rules that require additional disclosures.

Responses to consumer privacy requests

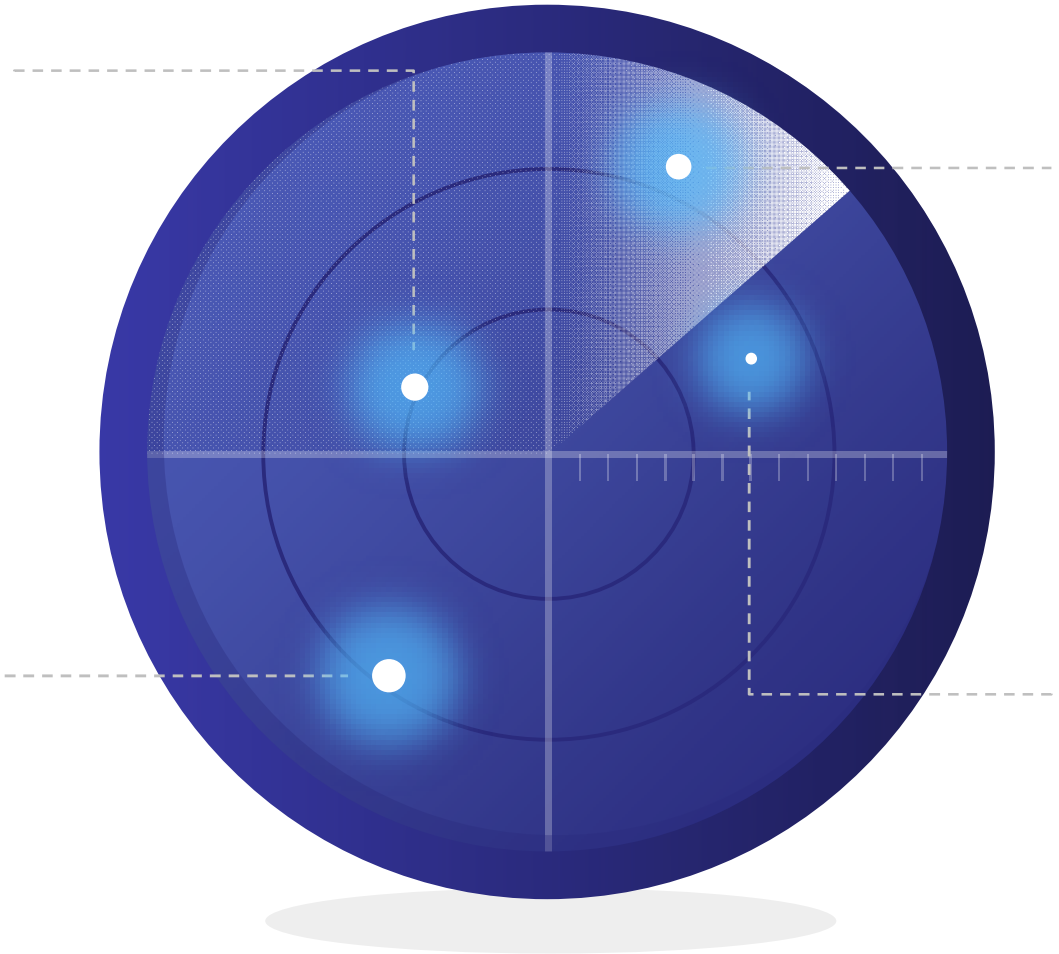
Privacy+ Security Forum

Regulator Radar-Privacy Requests

Privacy+ Security Forum

Notices

Are all applicable rights described adequately in the privacy policy?



Ease

How straightforward (or not) to make consumer privacy requests?

Follow Thru

Are requests honored and when not, are required disclosures made?

Timely

Are rights honored on time?

Responses are a signal of compliance

Privacy+ Security Forum

- Botched/ignored responses can lead to complaints to AGs
- Both CCPA actions have a Do Not Sell connection
  - But responses to other requests matter, too
- Pain points
  - Do Not Sell – “online” and “offline” opt-outs
  - Authorized agents and high-volume requests

How Do New AI-Related Obligations Affect Existing Privacy Rights Programs?

Privacy+ Security Forum

- **The AI Effect Part 2: Raising the Stakes for Privacy Rights Programs**

  - **Explainability—New Rights**
    - Colorado AI Law—Provide explanations of reasons, correction of inaccurate data, and appeals for adverse consequential decisions enabled by high-risk AI systems
    - Minnesota Consumer Data Privacy Act—Right to question results of profiling that have legal effect, obtain reason for result, correct inaccurate data on which decision is based, request reevaluation, and obtain information on actions to take to secure different decision
    - Draft CPPA Automated Decision-Making Technology Rules—Disclosures and access rights regarding the tool's logic and how the business used the output to make a decision

  - **Correction Rights**—How do you operationalize when an AI system has been trained on inaccurate data?

  - **Limitations on access and correction rights**—What happens when AI bills providing similar rights do not include the same exceptions?

  - **Impact on privacy governance**—Can you leverage existing processes to fulfill these obligations, or do you need to create new processes or hire additional personnel?

Tips

Privacy+ Security Forum

- Keep policies and processes up-to-date with new regulations
  - Add new rights (e.g., OR right to obtain list of third parties) promptly
  - Consider implications of AI-related obligations and how they affect scope of consumer rights, governance programs for processing and operationalizing rights, and disclosures.

- Test, and test again

- Document processes
  - CCPA requires 24-month retention of request records
  - Records *can* show mistakes are isolated lapses from strong practices

Key Takeaways

Privacy+ Security Forum

When you leave this room

Privacy+ Security Forum

Understand Your Data

Key areas of focus for regulators: Sensitive categories: Health, Children's

Governance

AI use & Websites must be managed proactively

Compliance Testing

A privacy notice and cookie banner are not cutting it anymore

Build your story

A defendable position should be the goal

Discussion

Privacy+ Security Forum

Speakers

Privacy+ Security Forum

Aaron Burstein

Partner
Kelley Drye & Warren
aburstein@kelleydrye.com

Shaundra Watson

Senior Director, Policy
BSA
shaundraw@bsa.org

Matt Dumiak

Director, Privacy Services
CompliancePoint
mdumiak@compliancepoint.com