

October 24, 2024

# Things that Go Bump In the Night: What are Privacy Dark Patterns?

**Kelly DeMarchis Bastide**  
Venable LLP

**Desarie Green**  
Cengage Group

**Lindsay Vogel**  
Bumble

# Speakers



## **Kelly DeMarchis Bastide**

Partner, Co-chair Privacy and  
Data Security Group  
Venable LLP



## **Desarie Green**

Sr. Privacy Counsel  
Cengage Group



## **Lindsay Vogel**

Lead Privacy Counsel  
Bumble

The background of the slide features a bokeh effect with numerous out-of-focus circles in shades of blue and green, set against a dark, almost black background. The circles vary in size and brightness, creating a soft, ethereal glow.

**What is a Dark Pattern?**

A solid, medium-blue horizontal bar spans the width of the slide, positioned below the main text.

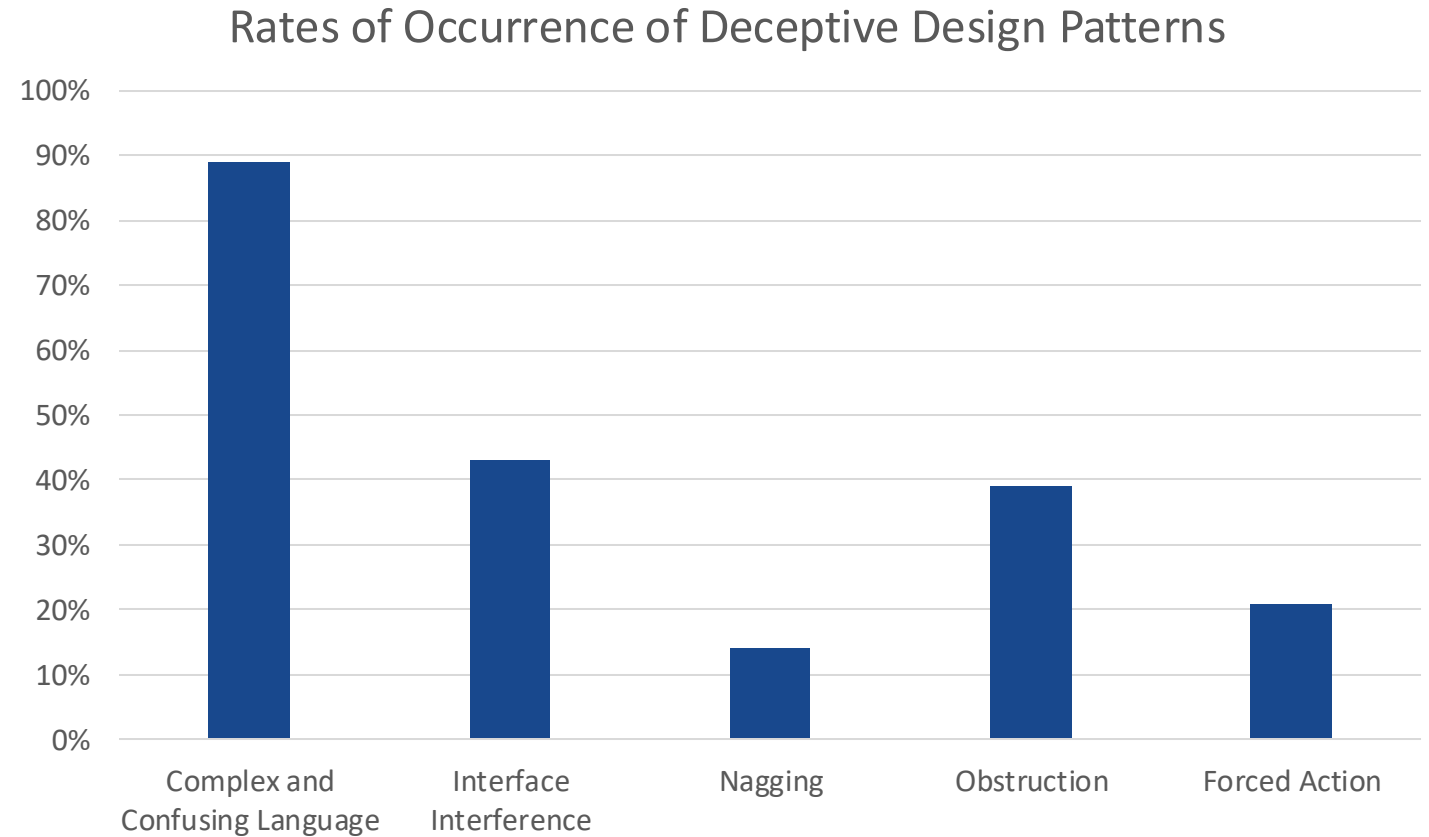
# What is a Dark Pattern?

**Dark Patterns** are deceptive or manipulative tactics used in online interfaces to influence user behavior, often at the expense of user privacy.

Legal Framework	Definition
<b>State Law Definitions</b> – California Consumer Privacy Act (CCPA), Colorado Privacy Act (CPA)	A user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice.
<b>Federal Trade Commission (FTC)</b>	Practices that trick or manipulate users into making choices they would not otherwise have made and that may cause harm.
<b>European Data Protection Board (EDPB)</b>	Interfaces and user experiences implemented on social media platforms that lead users into making unintended, unwilling and potentially harmful decisions in regards to their personal data with the aim of influencing users' behaviors.
<b>EU Data Act</b>	Design techniques that manipulate users into making decisions that have negative consequences.

# How Common are Dark Patterns?

The Global Privacy Enforcement Network (GPEN) found that an overwhelming 97% of websites and apps deploy at least one dark pattern to manipulate user behavior.



Source: GPEN Sweep 2024 "Deceptive Design Patterns"

# Why This Matters

Legal Framework	Key Provisions	Penalties/Enforcement
<b>California Privacy Rights Act (CPRA)</b>	Defines and prohibits dark patterns, invalidating consent obtained through dark patterns.	Fines up to \$2,500 per unintentional violation and \$7,500 per intentional or willful violation; enforced by the California Privacy Protection Agency (CPPA).
<b>Colorado Privacy Act (CPA)</b>	States that consent obtained through dark patterns is invalid.	Penalizes deceptive trade practices at \$20,000 per offense, capped at \$500,000.
<b>Federal Trade Commission (FTC)</b>	Focuses on misleading consumers, disguising ads, burying key terms, subscription barriers, and manipulating users into giving up data.	Settlements and fines, including over \$245 million in penalties in December 2022.
<b>General Data Protection Regulation (GDPR)</b>	Data protection laws interlinked with dark patterns where personal data is involved.	Maximum fines of €20 million or 4% of the organization's annual global turnover, whichever is greater.
<b>Digital Services Act (DSA) (EU)</b>	Article 25 explicitly bans dark patterns by prohibiting deceptive or manipulative online interface designs.	Fines of up to 6% of global turnover depending on number of active users.
<b>EU AI Act</b>	Prohibits the use of dark patterns in AI systems.	Up to €35 million or 7% of global revenue (whichever is higher, though lower penalty limits apply for SMEs) for prohibited AI practices, such as misleading, nudging, or using dark patterns.

# California Enforcement Advisory-- September



**CALIFORNIA PRIVACY  
PROTECTION AGENCY**  
ENFORCEMENT DIVISION

**ENFORCEMENT ADVISORY NO. 2024-02**

## **AVOIDING DARK PATTERNS: CLEAR AND UNDERSTANDABLE LANGUAGE, SYMMETRY IN CHOICE**

### **SUMMARY**

- Dark patterns harm consumers by subverting and impairing their autonomy, decisionmaking, or choice.
- Dark patterns are about effect, not intent.
- Using clear and understandable language and offering consumers symmetrical choices avoids impairing and interfering with consumers' ability to make their choice.

# California Enforcement, cont.

## QUESTIONS THE BUSINESS MIGHT ASK

As Business A reviews these user interfaces, it should ask itself the following questions consistent with 11 CCR §§ 7003(a) and 7004(a)(2) to determine whether: (1) the language is easy to understand and (2) the interfaces give consumers symmetrical choices:

- Is the language used to communicate with consumers **easy to read and understandable**?
- Is the language used **straightforward** and does it **avoid technical or legal jargon**?
- Is the consumer's path to saying "no" **longer** than the path to saying "yes"?
- Does the user interface make it **more difficult** to say "no" rather than "yes" to the requested use of personal information?
- Is it more **time-consuming** for the consumer to make the more privacy-protective choice?



# The FTC's "Click to Cancel" Rule

Announced  
Oct. 16th

## FACT SHEET

# The FTC's "Click to Cancel" Rule

This rule is helping the FTC get money back to people who are misled, and addressing common problems:

- ▶ Sellers who don't tell the truth or leave out necessary information.
- ▶ People who get billed when they didn't agree to pay.
- ▶ Sellers who make it hard — or impossible — to cancel.



### Under the FTC's amended Negative Option Rule:

- ✓ Important information must be truthful, clear, and easy to find.
- ✓ People have to know what they're agreeing to before they sign up.
- ✓ Sellers have to be able to show that people knew what they agreed to before they signed up.
- ✓ There always has to be a way to cancel that's as quick and easy as it was to sign up.
  - Sign up online? Click to cancel.
  - Signed up in person? Cancel online or over the phone.
- ✓ Violators can be liable for redress and civil penalties.

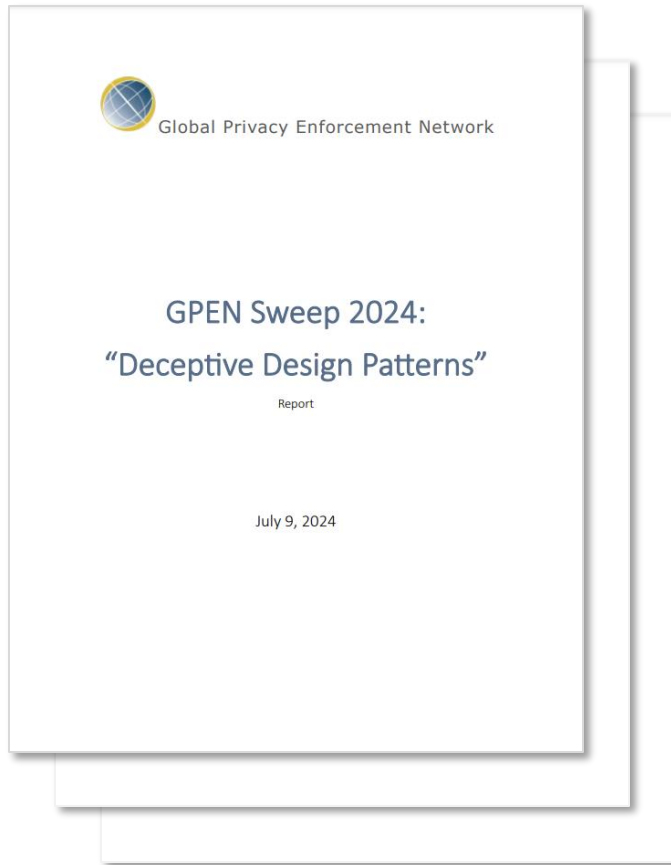


*The rule takes full effect 180 days after publication in the Federal Register.*

**Things That Go Bump  
in the Night...**



# GPEN's Taxonomy of Dark Patterns



**Complex and Confusing Language**



**Interface Interference**



**Nagging**



**Obstruction**



**Forced Action**

Using highly technical, convoluted, or legal jargon to mislead users, making it difficult for them to understand terms or conditions.



## Turning on the Lights with Best Practices



Use plain and simple language to help users understand the information so that they can provide informed consent.



Use layered privacy policies to enable users to control the level of detail they'd like to obtain.

# Our Very Long Website Privacy Policy

This very long website privacy concerns the processing of personal data provided or collected on the sites and applications where this privacy policy is posted, whether on our digital properties or on applications we make available on third-party sites or platforms. In some cases, we may provide additional data privacy notices specific to certain products, practices, or regions. Those terms are to be read in conjunction with this policy.

Pursuant to the laws that apply to the company, we collect information about users, guests, and others when they request or purchase products, services, or information from our company, create an account, interact with our products and services, visit our physical stores or properties, or otherwise interact with the company using one or more devices. We collect information through a variety of technologies, such as cookies, Flash cookies, pixels, tags, software development kits, application program interfaces, and Web beacons, including when you visit our sites and applications or use our applications on third-party sites or platforms using one or more devices, whether or not you are logged in or registered.

We may collect personal information and anonymous information. We may additionally use personal and anonymous information to create a third type of information, aggregate information.

Very long page

Not comprehensive

Vague legal references

Wall of text with no clear headings

Identifies the most recent policy update

Clear headings and formatting

Plain language that is easy to understand

A layered approach to access more details

Much shorter in length

# Website Privacy Policy

Last Updated: October 8, 2024

## What Information We Collect

We collect and store different types of information about you when you create an account, purchase our products, or interact with our website and app.  
[Learn more.](#)

## How We Use Your Information

We collect and use your information to provide you with our products and services, for marketing purposes, to improve our website, and to comply with the law.  
[Learn more.](#)

## How We Share Data & Why

We may share your information with third parties associated with the products purchased or services provided.  
[Learn more.](#)



# Interface Interference

The use of design elements and presentation methods that alter users' perception and understanding of their privacy options

## Examples of Interface Interference

- **“False hierarchy”** – emphasizing certain visual elements and obscuring others, thereby channeling users towards less privacy-protective options.
- **“Preselection”** – selecting by default more privacy-intrusive options.
- **“Confirm-shaming”** – using emotive language such that users gravitate towards options favored by the organization.



## Turning on the Lights with Best Practices



Present information in a fair, balanced way.



Adopt an opt-in approach where appropriate.



Use neutral, fact-based language.



# Interface Interference

**“False hierarchy”** – emphasizing certain visual elements and obscuring others, thereby channeling users towards less privacy-protective options.

Before you continue...

We use cookies to deliver the best possible user experience. When you visit our website, we may store and retrieve information on your browser, or access data like your IP-address or device information. [Privacy Policy](#).

Enhance my experience

Other choices

Accept &  
Continue

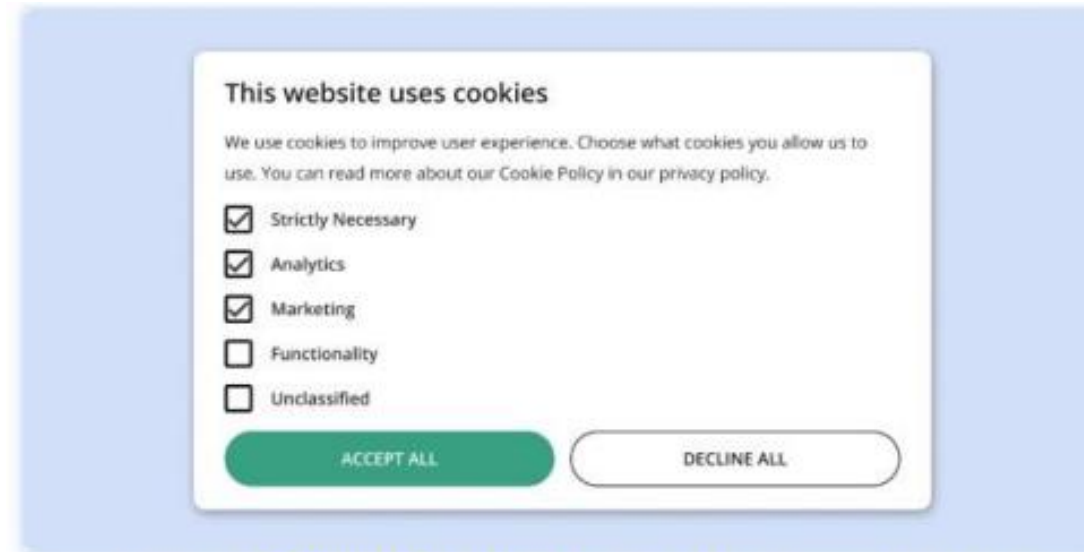
Manage  
Data Settings





# Interface Interference

**“Preselection”** – selecting more privacy-intrusive options by default.



CookieYes, [Dark Patterns in Cookie Consent](#), June 2024. CookieYes is a consulting company for cookie privacy compliance.



# Interface Interference

**“Confirm-shaming”** – using emotive language such that users gravitate towards options favored by the organization.

## Confirm Account Deletion

Are you really certain you want to delete your account? It would be a shame to see you go!

If you click “Delete User Account”, you will immediately lose all your VIP privileges.

Delete User Account

Save 15% off your first order!

Enter your email address here.

Confirm

*No, I hate saving money.*

Using repeated prompts or notifications that pressure users to take specific actions, often leading to annoyance.



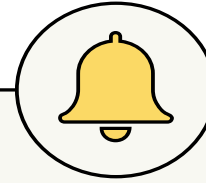
## Turning on the Lights with Best Practices



Limit number of reminders or prompts.




Provide clear and easy ways to dismiss or opt out of future notifications.



**You haven't logged  
in today!**

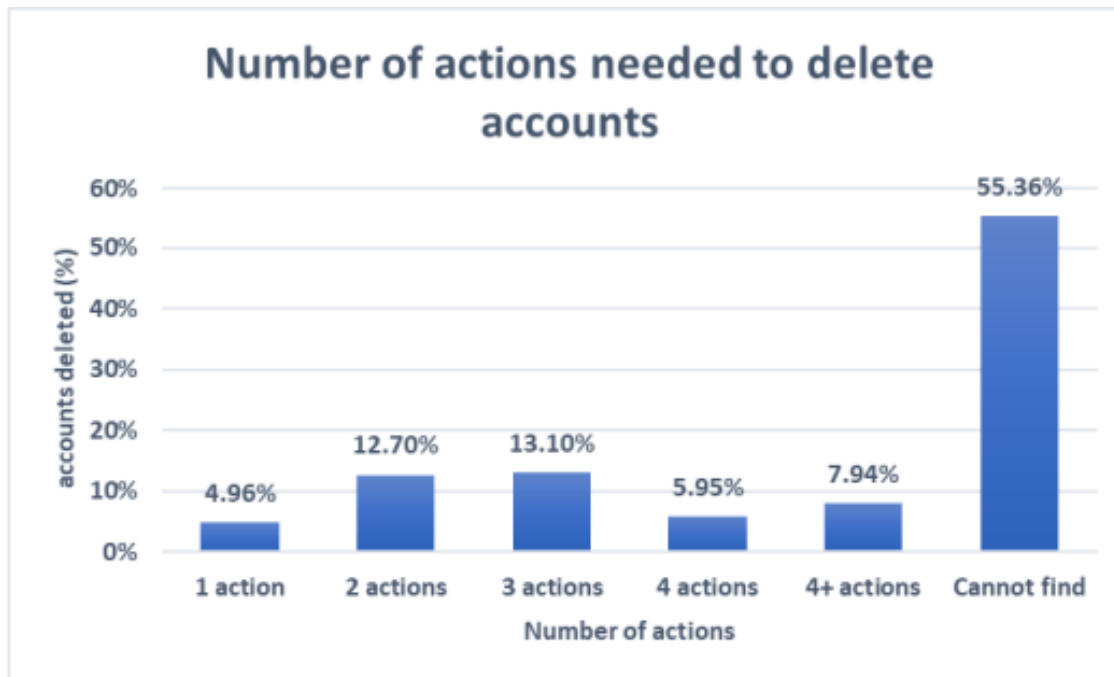


**Love our app?  
Share us with a friend!**

 Share

# Obstruction

Inserting additional steps between users and their goals, dissuading users from, or making them less motivated to, make their intended choices.



Source: GPEN Sweep 2024 “Deceptive Design Patterns”



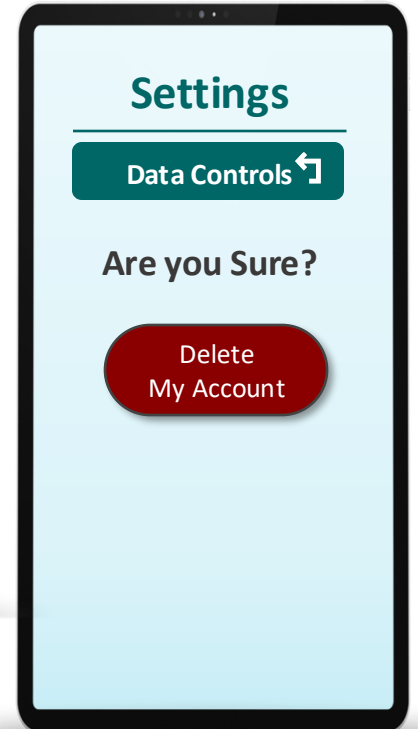
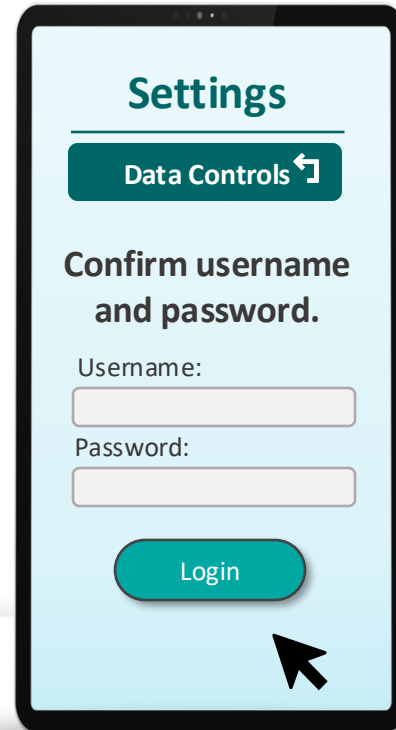
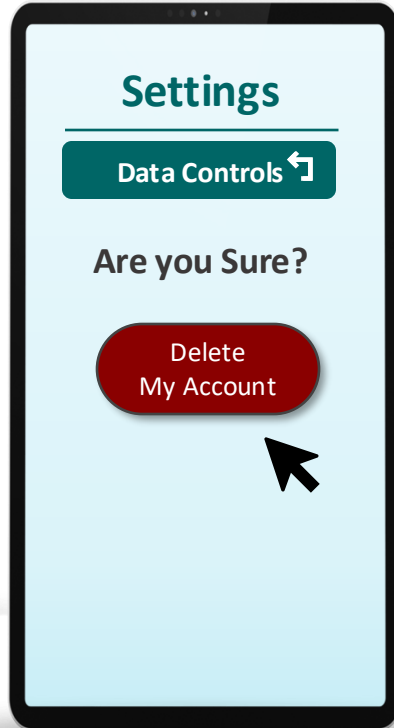
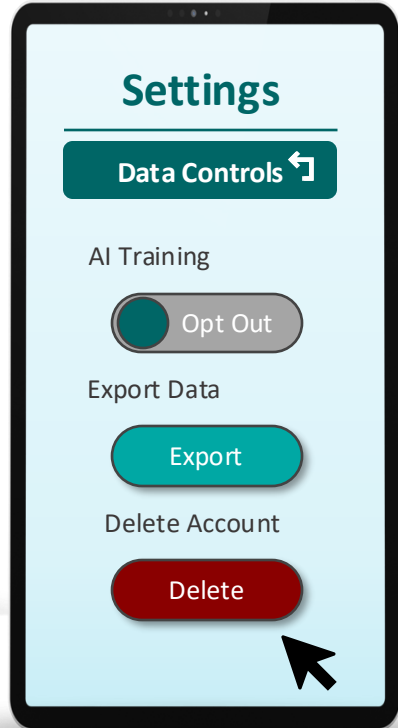
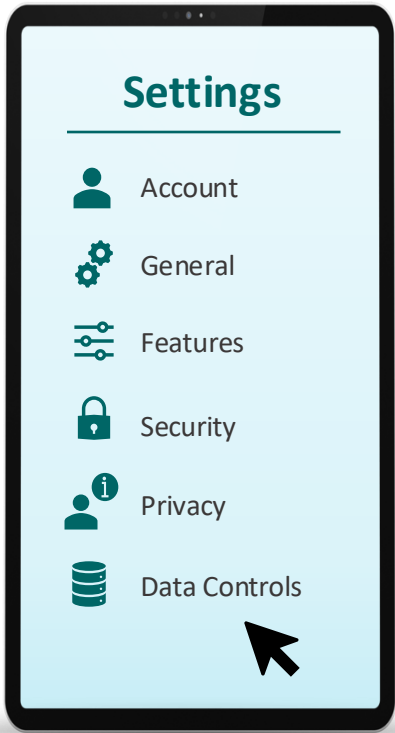
## Turning on the Lights with Best Practices



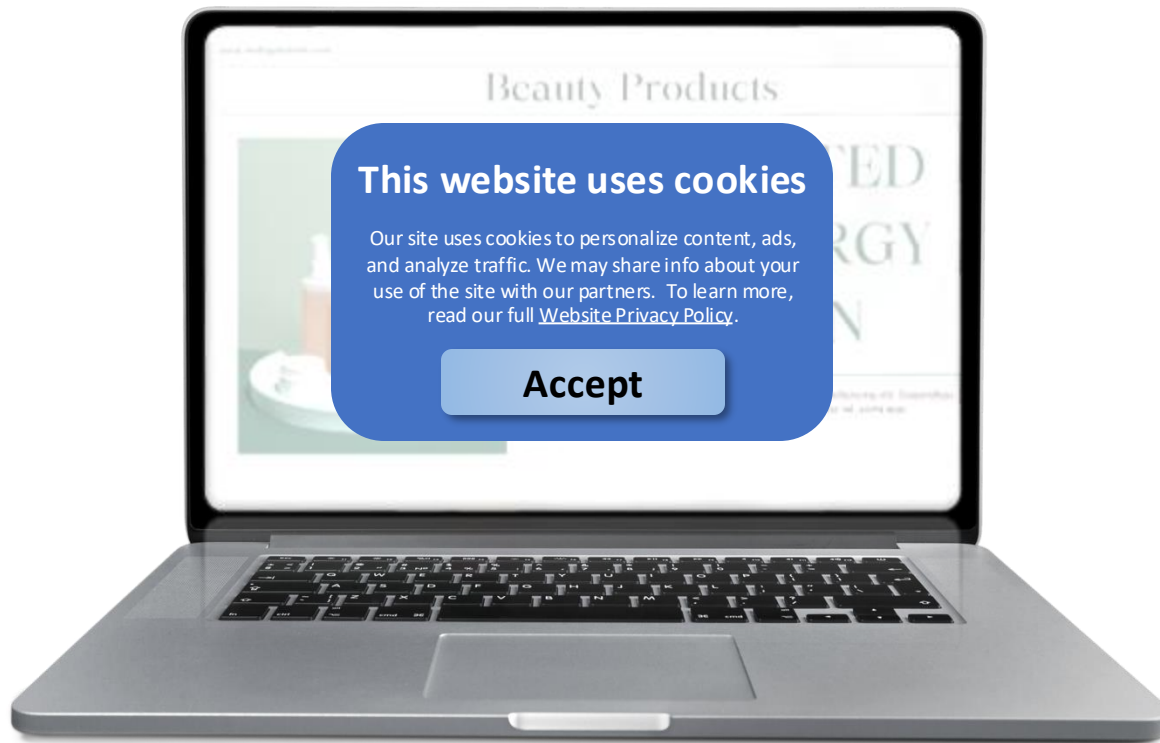
Make it easy for users to opt out or cancel.



Ensure processes only include necessary steps.



Services that put pressure on the user to complete the settings review at a time determined by the service provider without a clear option to postpone the process.



## Turning on the Lights with Best Practices



Provide users with choices about their personal data.



Don't force users to give up personal data unnecessarily.

**Don't be afraid**





# Conclusion



## Complex and Confusing Language



## Interface Interference



## Nagging



## Obstruction



## Forced Action



Use plain and simple language to help users understand the information so that they can provide informed consent.



Use layered privacy policies to enable users to control the level of detail they'd like to obtain.



Present information in a fair, balanced way.



Adopt an opt-in approach where appropriate.



Use neutral, fact-based language.



Limit number of reminders or prompts.



Provide clear and easy ways to dismiss or opt out of future notifications.



Make it easy for users to opt out or cancel.



Ensure processes only include necessary steps.



Provide users with choices about their personal data.



Don't force users to give up personal data unnecessarily.

Questions?



---

# Questions and Contacts



## **Kelly DeMarchis Bastide**

Partner, Co-chair Privacy and  
Data Security Group  
Venable LLP



## **Desarie Green**

Sr. Privacy Counsel  
Cengage Group



## **Lindsay Vogel**

Lead Privacy Counsel  
Bumble