

Eliminating Deceptive Privacy Practices: Building Trust by Addressing Privacy Dark Patterns



C O N T E N T S

4	Introduction
4	What Are Dark Patterns?
	5 / Why Are Dark Patterns so Common?
6	Why Should Enterprises Care?
6	Deceptive Patterns in Practice
	6 / Confusing Cookie Notices
	7 / Multiple-Click Cookie Banner
	9 / Complicated Privacy Settings
	9 / Lack of Interfaces on Internet of Things Devices
	10 / Manipulative/Confusing Language
	11 / Poor Interface Design
	12 / Forced Registrations
	12 / Inability to Change Settings
	13 / Default Settings
13	Addressing Deceptive Patterns
	13 / Privacy by Design
	14 / Know the User
	14 / Collaboration: The Key to Eliminating Dark Patterns
	14 / UX
	14 / Marketing
	15 / Simplifying the User's Privacy Experience
	16 / <i>Deceptive Patterns at Small-to-Medium Enterprises</i>
17	Putting This Into Practice
17	Conclusion
18	Acknowledgments

A B S T R A C T

Privacy dark patterns are deceptive tactics that trick or manipulate consumers into sharing more data than they may prefer. Many enterprises employ dark patterns despite the fact that they erode digital trust, increase risk and cause harm. This white paper explores why dark patterns are both common and problematic and provides real-world examples and strategies to replace them in favor of better, more consumer-centric alternatives.

Introduction

Many consumers say they want privacy, but their actions often do not reflect that desire.¹ This paradox may be partially attributed to a variety of factors, including a lack of awareness or understanding of the digital world and the reluctance to review lengthy or complex privacy notices before using a digital product or service.² It may also be due to the difficulty of limiting the collection and use of personal information or requesting not to be tracked. Individuals also encounter numerous data-sharing requests daily. As a result, they may experience consent fatigue and accept these requests without considering if they align with their privacy preferences.³

Many websites and applications track users by default to provide a better user experience, but it can be very difficult to opt out of, or limit, that tracking.

Enterprises with complicated privacy settings and confusing privacy interfaces engage in dark patterns. These practices can significantly affect their reputation and the trust earned from consumers. But privacy professionals can work closely with user experience (UX) designers to avoid these concerns, creating a truly privacy-centric experience for consumers.

What Are Dark Patterns?

Enterprises may leverage dark patterns to “trick or manipulate consumers into buying products or services or giving up their privacy.”⁴ Dark patterns are practices that make it difficult for system/product users to understand and express their privacy preferences. In some instances, developers will intentionally design interfaces or practices to incentivize users into spending money or oversharing data.

For example, the US Federal Trade Commission (FTC) recently took action against Amazon, claiming that it manipulated consumers into enrolling in Amazon Prime memberships that automatically renew. The FTC alleged that Amazon intentionally engaged in a variety of dark

patterns, from making it difficult to purchase items without an Amazon Prime subscription to deceiving consumers into purchasing a subscription when completing their transactions and creating a deliberately complicated process for canceling a subscription.⁵

Dark patterns are not just about getting users to spend money; they can also be about deceiving users into sharing their personal information. Privacy dark patterns, interchangeably referred to as “deceptive patterns” in this paper, are methods of tricking or nudging people to act in ways that may not align with their privacy preferences.

1 John, L.; “We Say We Want Privacy Online, But Our Actions Say Otherwise,” *Harvard Business Review*, 16 October 2015, <https://hbr.org/2015/10/we-say-we-want-privacy-online-but-our-actions-say-otherwise>

2 Griffith, E.; “Everyone Wants Data Privacy, But No One Reads Privacy Agreements,” *PC Mag*, 19 April 2021, <https://www.pcmag.com/news/every-one-wants-data-privacy-but-no-one-reads-privacy-agreements>

3 Schermer, B.; B. Custers; S. Van der Hof; “The crisis of consent: How stronger legal protection may lead to weaker consent in data protection,” *Ethics and Information Technology*, vol. 16, iss. 2, May 2014, https://www.researchgate.net/publication/271922021_The_crisis_of_consent_How_stronger_legal_protection_may_lead_to_weaker_consent_in_data_protection

4 US Federal Trade Commission (FTC), “FTC Report Shows Rise in Sophisticated Dark Patterns Designed to Trick and Trap Consumers,” 15 September 2022, <https://www.ftc.gov/news-events/news/press-releases/2022/09/ftc-report-shows-rise-sophisticated-dark-patterns-designed-trick-trap-consumers>

5 FTC, “Federal Trade Commission v. Amazon.com, Inc.,” 21 June 2023, https://www.ftc.gov/system/files/ftc_gov/pdf/amazon-rosca-public-redacted-complaint-to_be_filed.pdf

These methods often manifest in poor user design, difficult-to-find or -understand privacy settings, confusing wording, and time-consuming opt-out processes.

As a privacy-specific example, in 2022, Google entered into a US \$85 million settlement due to the alleged use of privacy dark patterns. The lawsuit alleged that Google tracked user locations in the background of its Android mobile phones even after users turned off the location tracking functionality. Additionally, the suit said privacy settings were hard to find.⁶

These are just a few examples, and the use of deceptive patterns is increasing.⁷ Enterprises must prevent these practices from becoming normal or acceptable. An enterprise that respects users and empowers them to express their privacy preferences can earn consumer trust and gain a competitive advantage over their peers who do not respect for data subjects.

Why Are Dark Patterns so Common?

Many enterprises believe that data is the most valuable strategic asset in the modern world. Data can provide significant insights into consumer buying trends and reveal information that can improve target marketing and advertising, which drives sales and revenue. But the path to more data can simultaneously create an increased reliance on dark patterns under the mistaken theory that more is better.

Marketing professionals who rely on personal information to tailor advertising are not privacy experts; they may complete enterprisewide privacy awareness training that primarily addresses compliance-related concerns, but their primary job focus is not digital trust. Because of that, privacy professionals must take a leading role in collaborating with these teams to better balance potentially competing interests and empower everyone to champion privacy.

Marketing teams are not solely responsible for the rise in deceptive patterns. Any department that creates online products, services or consumer-facing content (e.g., designs websites); creates email copy; or develops applications can inadvertently employ deceptive patterns. In many enterprises, privacy professionals may be siloed from these departments or engaged downstream, and their lack of engagement can spark the creation of deceptive patterns.

While global privacy laws and regulations have helped protect data subjects' privacy, they may also be a contributing factor to the rise in the use of deceptive privacy patterns. According to one estimate, the General Data Protection Regulation (GDPR) is responsible for an almost 40 percent increase in cookie consent notices.⁸ While seemingly innocuous, these notices are often a main source of deceptive patterns, such as not having a clear "reject" button. Though laws and regulations have required enterprises to provide notice and obtain consent to collect personal data, they may have inadvertently nudged enterprises to gather data more creatively (or deceptively).

While global privacy laws and regulations have helped protect data subjects' privacy, they may also be a contributing factor to the rise in the use of deceptive privacy patterns.

It is important to note that not all deceptive patterns are intentional. For example, poor UX design, such as using colors that are difficult to read, can lead to dark patterns. Although privacy impact assessments should be performed before collecting data for a new purpose and before a new product or service is released, it is possible some marketing emails or website copy may still leverage dark patterns. Because privacy teams do not frequently work with copywriters or web designers, these patterns can go unidentified or untested.

6 Weatherbed, J.; "Google will pay \$85M settlement to Arizona to end user-tracking suit," The Verge, 5 October 2022, <https://www.theverge.com/2022/10/5/23389331/google-settlement-arizona-user-tracking-privacy-suit>

7 *Op cit* US FTC

8 Kretschmer, M.; J. Pennekamp; K. Wehrle; "Cookie Banners and Privacy Policies: Measuring the Impact of the GDPR on the Web," *ACM Trans. Web*, vol. 15, iss. 4, Article 20, June 2021, <https://www.comsys.rwth-aachen.de/fileadmin/papers/2021/2021-kretschmer-tweb-cookies.pdf>

Why Should Enterprises Care?

Even though the use of deceptive patterns is common, enterprises should focus on establishing and maintaining trust with consumers. At best, individuals will feel frustrated when they realize they have been tricked into providing personal information. At worst, they will choose another provider offering an identical or similar service.

New privacy laws and regulations specifically address the use of dark patterns. In the United States, California was the first state to prohibit using dark patterns to obtain consent.⁹ And while the GDPR did not initially call out dark patterns, lawmakers have indicated that further legal guidance will be provided to address them.¹⁰ Ultimately, it is possible that laws and regulations will prohibit the use of dark patterns in the future, but enterprises should be proactive given the clear regulatory signals, including enforcement actions that have already been taken.

Preventing deceptive patterns can also support other enterprise goals and values. Many enterprises have

prioritized diversity, equity and inclusion (DEI) in recent years, with 95 percent of chief executive officers expressing in a survey that DEI is a priority for their companies over the coming years.¹¹ However, it is paradoxical to claim to value DEI while using dark patterns.

Deceptive patterns are likely to cause more harm to marginalized groups, especially individuals with lower incomes and lower levels of education.¹²

A high level of education or technical skills should not be a prerequisite to privacy.

Dark patterns may also disproportionately affect those with less technical literacy and those who do not speak English as a first language in a country where English is the primary language.¹³

A high level of education or technical skills should not be a prerequisite to privacy. Enterprises must work to provide all individuals, regardless of background, equal opportunity to act on their privacy preferences.

Deceptive Patterns in Practice

Privacy dark patterns can appear in a plethora of ways, and at different times, in a user's journey. The following are some of the most common deceptive patterns and approaches to addressing them.

Confusing Cookie Notices

Many websites have notices that ask visitors for permission to collect cookies. These cookie notices should be easy to understand and use clear language.

9 The California Privacy Rights Act of 2020, https://oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf

10 Cooper, D.; S. Jungyun Choi; J. Ong; A. Oberschelp de Meneses; "The EU Stance on Dark Patterns," Inside Privacy, 31 January 2023, <https://www.insideprivacy.com/eu-data-protection/the-eu-stance-on-dark-patterns/>

11 Hawkins, D.; "How CEOs Can Make Diversity And Inclusion A Priority," *Forbes*, 13 July 2022, <https://www.forbes.com/sites/forbescoachescouncil/2022/07/13/how-ceos-can-make-diversity-and-inclusion-a-priority/?sh=463abf3e279a>

12 Busch, K.; "What Hides in the Shadows: Deceptive Design of Dark Patterns," Congressional Research Service, 4 November 2022, <https://sgp.fas.org/crs/misc/IF12246.pdf>

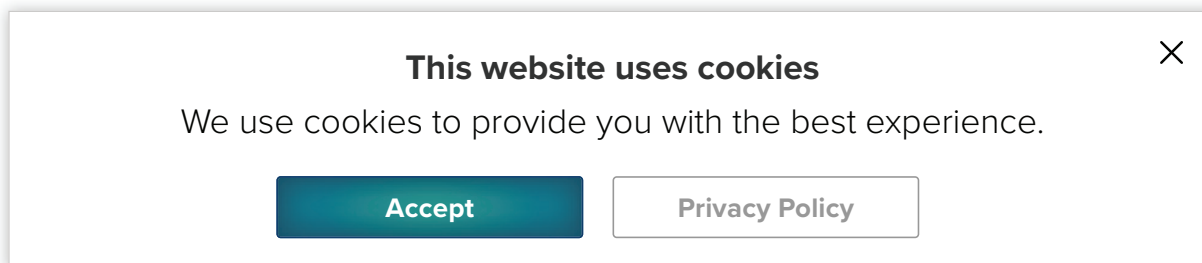
13 Germain, T.; "New Dark Patterns Tip Line Lets You Report Manipulative Online Practices," Consumer Reports, 19 May 2021, <https://www.consumer-reports.org/digital-rights/dark-patterns-tip-line-report-manipulative-practices-a1196931056/>

The ePrivacy Directive, which supplements the GDPR, requires websites to obtain consent before storing cookies in the user's browser (except for "strictly necessary" cookies).¹⁴ Deceptive patterns are especially

common in cookie notices partially because there is no regulatory guidance on how one should be crafted.

Figure 1 shows an example of a confusing cookie notice.

FIGURE 1: Confusing Cookie Notice



The cookie notice in **figure 1** is misleading and may cause users to draw inaccurate conclusions about the information being collected. There is no obvious "reject" button. Users may believe that their options are to accept cookie tracking or read the privacy policy and then accept cookie tracking.

Though there may be a way to decline cookies by clicking on the "Privacy policy" button, many users will not know it is possible or want to navigate the settings in order to decline cookie tracking.

To address this deceptive pattern, enterprises should ensure cookie banners are as easy to understand as possible. In addition to an "accept" button, there should be a button to reject cookies.

The wording on this button should make it clear that users do not have to accept cookies to use the website. Ensure the button looks like a clickable button; some

cookie banners make the reject button gray, creating the appearance that it cannot be clicked.

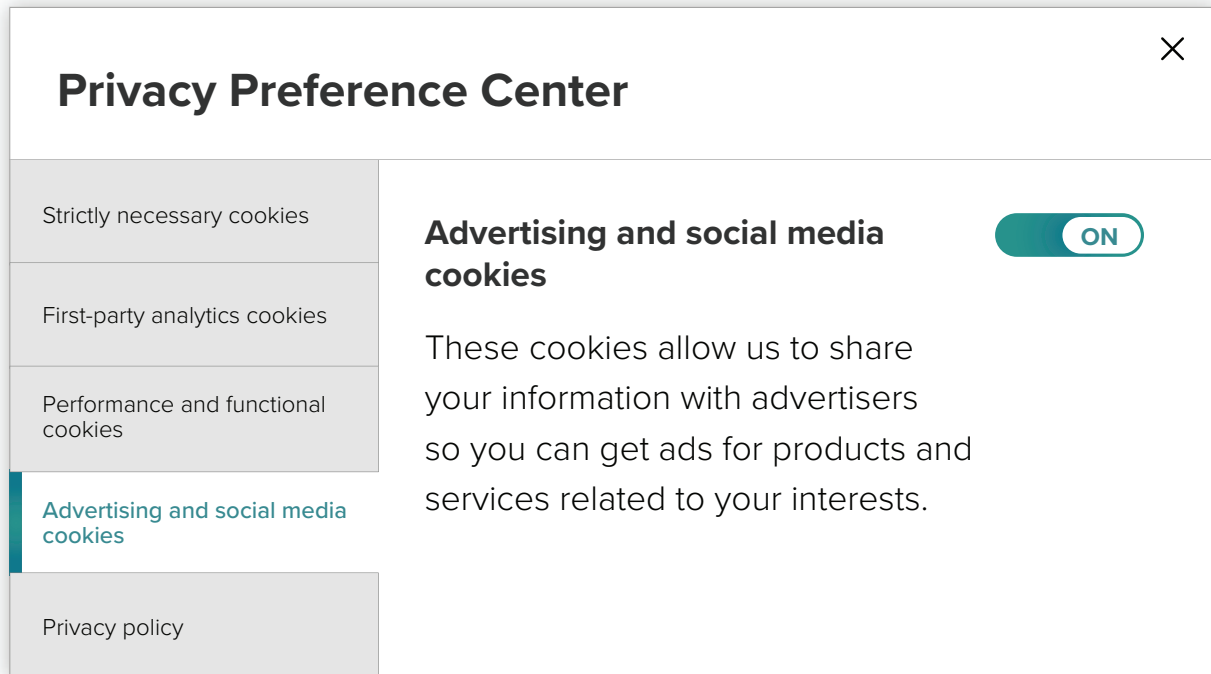
Multiple-Click Cookie Banner

Some cookie banners require users to click multiple times to reject cookies, while accepting cookies requires just one click. Though a few clicks may not seem significant, the additional time and friction is often intentionally designed to guide users down the path of less privacy. **Figure 2** shows a cookie banner that requires multiple clicks to reject cookies.

Website visitors may find the cookie banner in **figure 2** frustrating because it requires at least four clicks, not including the toggles, to change the default settings.

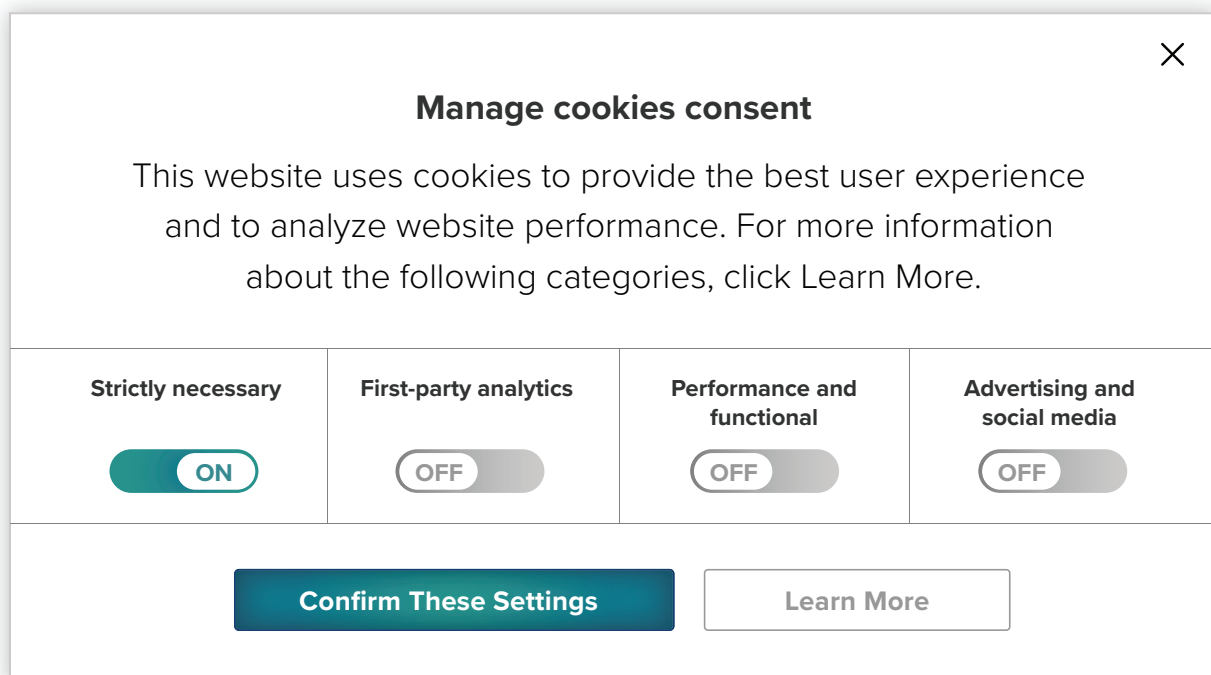
If it takes multiple clicks to reject tracking but only one click to accept all tracking, many users may accept all cookies rather than spend time setting and confirming their true preferences across multiple pages.

14 GDPR.EU, "Cookies, the GDPR, and the ePrivacy Directive," <https://gdpr.eu/cookies/>

FIGURE 2: Multiple-Click Cookie Banner

Providing granular cookie preferences is valuable, but there is a better way to present the information. Checkboxes for each tracking category on the initial cookie banner allow users to confirm their choices

with fewer clicks. **Figure 3** shows a cookie banner that allows website visitors to express their cookie-tracking options without having to click on multiple tabs or menus. Additionally, superfluous tracking is unchecked by default.

FIGURE 3: Cookie Banner With Categories

Complicated Privacy Settings

Cookie banners are only one area where dark patterns appear. They can also be found in complex, difficult-to-navigate menus that hide privacy settings. It is imperative to have accessible privacy settings, as privacy notices are often ignored due to their length and density. The average American has 80 applications (apps) on their phone.¹⁵ It would take 22.4 hours to read all the related privacy policies,¹⁶ and that does not include browsed websites. Given these challenges, users may find it easier to modify their privacy choices rather than reviewing lengthy privacy policies.¹⁷ For this reason, it is crucial that enterprises make privacy settings easy to find.

The following are some ways in which privacy settings can be hidden:

- Only one difficult-to-find tab on the preferences page allows users to modify their settings.
- Privacy settings are on a page that does not mention privacy (e.g., a security settings page).
- Privacy-related settings are distributed across a few preference pages rather than in a central location where a user can modify them.

One of the most effective ways to address this issue is to provide several paths for accessing privacy settings.¹⁸ For example, the privacy settings page may

be accessible through a user's profile page, the settings page and the privacy link at the bottom of a webpage. It is also worthwhile to have a frequently-asked-questions page with instructions on how to access privacy settings and to train customer service staff on how users can find these settings.

Lack of Interfaces on Internet of Things Devices

Internet of Things (IoT) devices, such as fitness trackers and smart appliances, sometimes collect granular and sensitive information. But because many IoT devices do not have screens like phones and computers do, it might not be easy to access privacy settings, or there may not be a mechanism to address privacy preferences. In fact, some IoT devices do not even have privacy policies. (There may be policies for the product's website or associated app but no policies specific to the device and the data it collects.)

Figure 4 illustrates some common IoT device categories, the data that may be collected and the inferences that can be made about users based on the collected data. Note that the data collected by IoT devices can vary from device to device.

FIGURE 4: IoT Devices and the Data They Collect

IoT Device Category	Data Collected	Possible Conclusions From Data
Fitness trackers	Heart rate, sleep pattern, steps taken	A person's heart rate may indicate their stress level. Trends over time may indicate an individual's routine, e.g., when that person sleeps.
Video doorbells	Video recordings, audio recordings	Video recordings may capture the facial features of neighbors and visitors of a home. These recordings could be shared with local law enforcement.
Entertainment streaming devices	Channels/programs watched, duration of streaming	Channels/applications watched may indicate the demographics of a household, interests and political views.
eReaders	Books purchased, location	Books purchased may reveal information about a person's orientation, political beliefs or health conditions.

15 Flynn, J.; "40 Fascinating Mobile App Industry Statistics [2023]: The Success of Mobile Apps in the U.S.," Zippia, 20 March 2023, <https://www.zippia.com/advice/mobile-app-industry-statistics/#~:text=The%20average%20American%20has%2080,app%20downloads%20worldwide%20in%202020>

16 Fowler, G.; "I tried to read all my app privacy policies. It was 1 million words," *The Washington Post*, 31 May 2022, <https://www.washingtonpost.com/technology/2022/05/31/abolish-privacy-policies/>

17 Kcick, D.; "Finding privacy choices on websites is hard for average users," CyLab, 11 June 2020, <https://www.cylab.cmu.edu/news/2020/06/11-privacy-choices-websites.html>

18 *Ibid.*

Given the information that can be gathered—and the conclusions that can be drawn—from data collected by IoT devices, it is crucial to enable consumers to easily modify IoT privacy settings when initially setting up the device and downstream.

Additionally, enterprises should have privacy policies specific to the device, associated app and website. It is not sufficient to only have a policy for an IoT device's app and not highlight the information collected and used by the device.

Manipulative/Confusing Language

Some requests for information rely on manipulative language. For example, a retail website may ask customers for email addresses for promotional emails, and a customer can either enter their email address or click a link that says something like, “I hate saving money” (**figure 5**). In addition to manipulative language, it may be ambiguous to the users whether they can access the website without providing an email address because the decline option is not obviously a button.

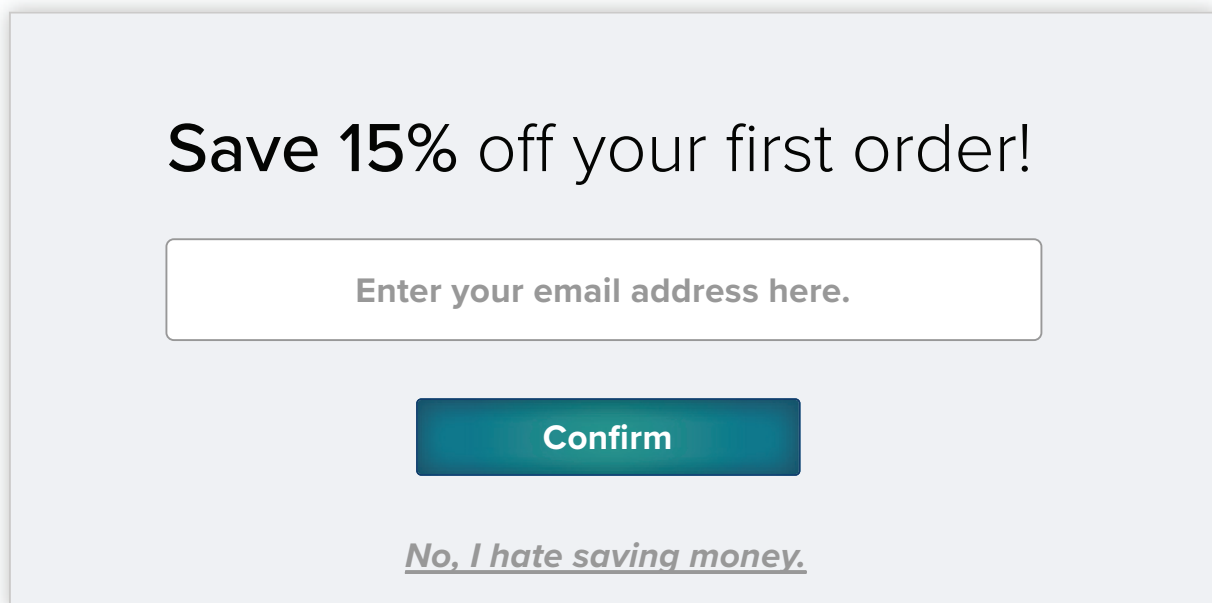
Some consent requests leverage confusing language to manipulate users, making it unclear what users are agreeing to. This deceptive pattern can be avoided by ensuring it is clear that users do not have to provide an email address to access a website. This means making the “decline” button as easy to see as the button to share information.

Additionally, the option to not provide information should not have judgment in it; a button that instead says “Decline,” for instance, allows users to opt out of sharing information without any pressure.

This dark pattern may also entail grouping necessary functional cookies with optional tracking cookies, leading users to believe this kind of tracking is necessary for the website to function properly.

To avoid confusing language that leads to deceptive patterns, ensure that the department responsible for creating this copy shares it with privacy and UX teams for review.

FIGURE 5: Manipulative Language in Email Collection Requests



Save 15% off your first order!

Enter your email address here.

Confirm

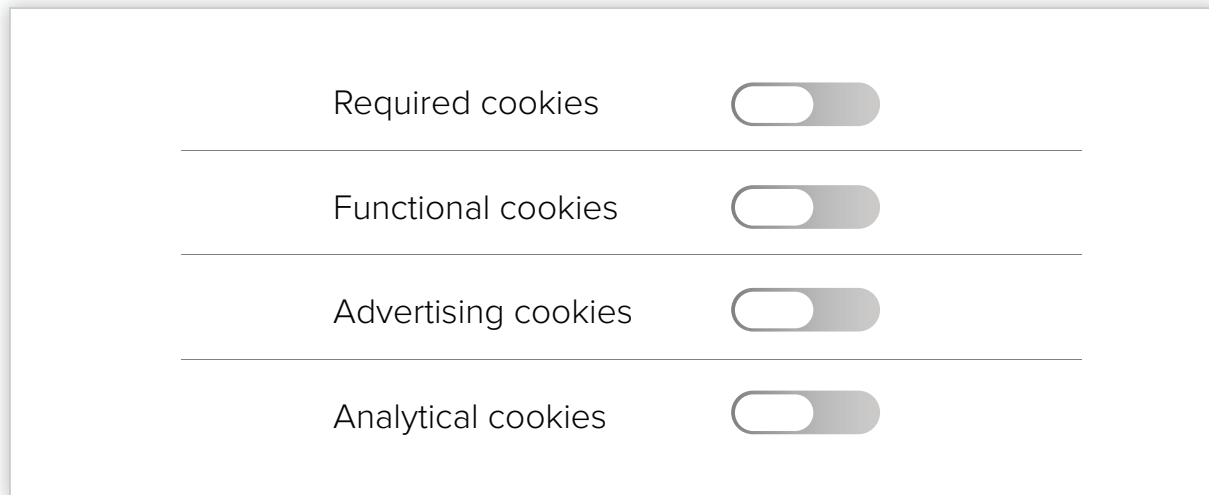
No, I hate saving money.

Poor Interface Design

Privacy-related web interfaces may be designed in a way that deliberately tricks users into sharing their personal information. This can happen when toggles are difficult

to interpret or lack contrast. Because the toggles in **figure 6** do not utilize a strong contrast or bold color to indicate what is or is not allowed, users may quickly glance at it and assume that functional, advertising and analytical cookies are not being tracked.

FIGURE 6: Confusing Toggles

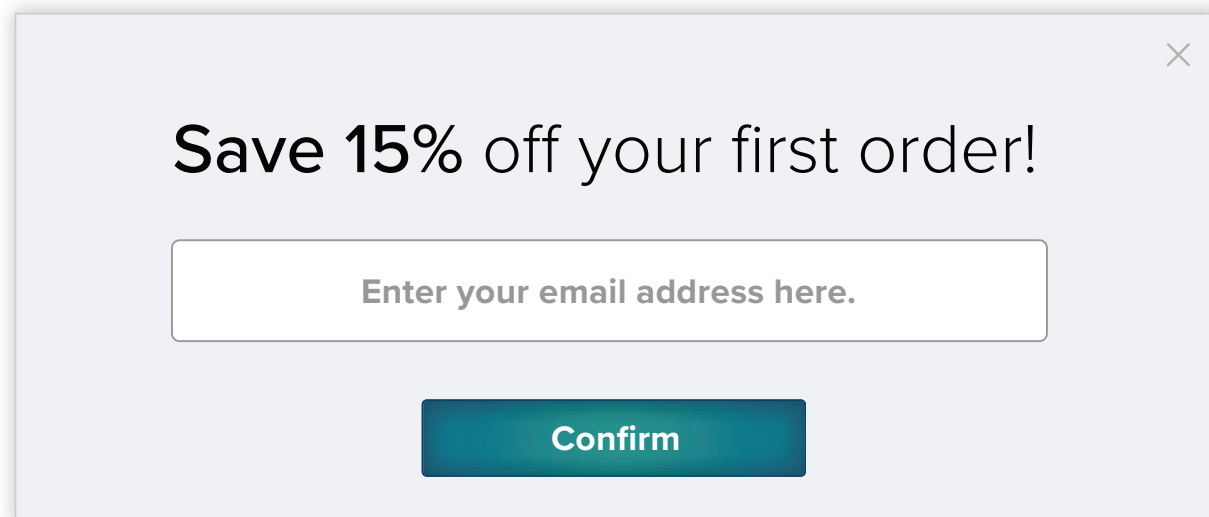


To address this deceptive pattern, be sure that toggles use color to indicate when tracking is enabled. It may also be useful to have the word “on” next to any enabled toggles, allowing users to confirm that they are selected.

pop-up with a small, hard-to-see “x” in the top-right corner. Because there is little contrast, users may not know that providing their email address is optional and may think they need to provide it to access the website. This can easily be addressed by using more contrast, leveraging UX best practices and conducting extensive testing before deploying in production.

Poor interface design can also result in pop-ups with difficult-to-see “close” buttons. **Figure 7** shows a

FIGURE 7: Close Button



Some interfaces also make it ambiguous as to what option is selected in the cookie banner. For example, if the “accept” and “reject” buttons turn colors when clicked, it may not be clear whether the color indicates

the option is selected. To address this issue, clarify to users which option is selected. This can be done by using text in addition to color to eliminate any ambiguity.

Email unsubscribe links often employ deliberately poor design to keep people subscribed. Some promotional emails may not include an easy-to-find unsubscribe link in the message. Additionally, unsubscribe pages sometimes leverage confusing wording, making it difficult to opt out of future communications.

For instance, an email's unsubscribe page may say, "Are you sure you want to unsubscribe?" with "No" as the prominent, highlighted choice and "Yes" in smaller text below. To address this dark pattern, ensure that all options are given a similar design treatment and the colors are not nudging users to make a certain choice.

Forced Registrations

Forced registration requires users to create an account and provide personal information to access information, service or a product. While certain information may be needed to complete a transaction, such as an email address for an order confirmation, enterprises should not require users to create accounts.

If, for some reason, it is necessary to have users create accounts, limit the amount of information collected.

For example, do not require users to have a credit card stored on their account, do not require a physical mailing address if products are not mailed to users, etc. If users are required to create accounts, clearly explain how this information will be used.

Inability to Change Settings

Some enterprises make it difficult to change privacy-related settings. These settings might be clearly presented, but users cannot modify them, e.g., requiring an email address to download a resource (**figure 8**).

The requirement in **figure 8** is considered a privacy dark pattern because it forces users to share their information with third parties.

Sharing information with third parties is not essential to the functionality of a user making a purchase. Therefore, there is no legitimate reason why third-party sharing should be required in this case.

Some websites also leverage the inability to change settings for cookie-tracking purposes. For example, a cookie banner may only have the option of accepting cookies or learning more, and the learning more link does not provide users with a way to opt out of tracking.

This differs from the deceptive pattern involving confusing cookie banners, as a confusing cookie banner may still allow users to opt out of tracking.

To address this dark pattern, practice the principle of data minimization, i.e., collecting the least amount of information necessary. Enterprises must know what data are needed for a particular service and how those data will be used. Superfluous data should not be collected.

FIGURE 8: Inability to Change Settings



By clicking this box, you agree to have your information shared with third parties, including advertisers.

This field is required.

Purchase Now

Default Settings

Some enterprises rely on data subjects not knowing how to, or not caring to, change default privacy settings. The default setting may not be privacy preserving, and users who do not change their settings may share more

information than they would prefer. If the checkbox in **figure 8** were automatically checked, that would exemplify the deceptive pattern of nonprivacy preserving default settings. Practicing privacy by design can help reduce dark patterns resulting from default settings.

Addressing Deceptive Patterns

Privacy dark patterns are pervasive and can exist in numerous interactions between enterprises and individuals. Privacy by design and cross-functional collaboration can help prevent deceptive patterns and limit harm to data subjects.

Privacy by Design

Privacy by design, which integrates full-sum privacy into the entire development life cycle (including implementation and use), can help address dark patterns and limit the harm caused by inadvertently deceptive design. The following are the seven principles of privacy by design:¹⁹

- **Proactive, not reactive; preventative, not remedial**—Privacy professionals should remediate dark patterns before receiving complaints; by that point, reputational damage and loss of trust have already occurred, and it may not be possible to recover. Instead, proactively work to identify and eliminate any dark patterns through collaboration with other departments and privacy impact assessments for new developments.
- **Privacy as the default setting**—If systems and websites are configured to protect privacy by default, the harm caused by inadvertent dark patterns will be limited. Even if it is difficult for users to find or modify their privacy-related settings, their tracking preferences should default to protecting privacy, and action is needed for users to share information. Operate from the mindset of data subjects needing to opt into data sharing rather than opt out of sharing data.
- **Privacy embedded into design**—Privacy professionals can enlist the help of UX designers to ensure that user preferences in the design support privacy. This includes the mechanism by which

consumers can set their privacy preferences and the default data collected by systems and products. This principle can help eliminate dark patterns associated with forced registration, IoT interface limitations, poor interface design and the presentation of privacy-related settings.

- **Full functionality: Positive-sum, not zero-sum**—This principle can ensure that useability, functionality and profitability are compatible with privacy. Enhanced privacy must be compatible with business objectives. Ultimately, privacy should be a core functionality consideration, and systems and websites should be designed to operate with the least amount of user information necessary. This principle can help eliminate dark patterns associated with IoT interfaces, forced registration and the inability to change settings.
- **End-to-end security: Full life cycle protection**—This principle ensures that the information consumers provide is adequately protected. If dark patterns are collecting more data than is strictly necessary, strong security measures can protect the information that an enterprise has, limiting the harm to individuals.
- **Visibility and transparency: Keep it open**—Dark patterns are antithetical to this principle. Enterprises that are honest and transparent about the data they collect and how those data will be used cannot leverage deceptive patterns. Note that this transparency is not just about the front-end that users see; it is also about the data processing and sharing occurring on the backend that users do not see. This principle can help address deceptive patterns associated with manipulative language and confusing cookie banners.
- **Respect for user privacy: Keep it user-centric**—Designing with users (and not just their data) in mind ensures that individuals can indicate their privacy preferences and act to protect their privacy. Ultimately, all intentional deceptive patterns can be remediated by respecting the user and designing with them in mind.

¹⁹ Cavoukian, A.; "Privacy by Design—The 7 Foundational Principles," January 2011, <https://www.ipc.on.ca/wp-content/uploads/resources/pbd-implementation-7found-principles.pdf>

Know the User

Addressing deceptive patterns requires knowing who an enterprise's users or potential users are. Their abilities,

preferences and background will greatly influence how an enterprise should present its privacy obligations and settings. **Figure 9** contains some categories of demographic information and associated privacy considerations.

FIGURE 9: Demographics and Privacy Considerations

Demographic Information	How it May Affect Privacy
Age	<ul style="list-style-type: none"> Additional privacy considerations may be needed for processing the data of minors. Digital natives may find it easier to access and modify settings than those who did not grow up with digital technologies.
Region	<ul style="list-style-type: none"> Additional privacy considerations may be needed for users from certain areas. Privacy notices may need to be provided in multiple languages to ensure all users can understand them. Cultural considerations may affect the overall look and design of privacy settings (e.g., the cultural connotations of certain colors).
Ability	<ul style="list-style-type: none"> Privacy settings must account for accessibility (e.g., accommodating colorblindness). Privacy notices must be conveyed to users in a meaningful and understandable way.

Most demographic information can be obtained from an analytics and performance measurement program. To get to know the user, privacy professionals must enlist the help of the UX team.

Collaboration: The Key to Eliminating Dark Patterns

Privacy professionals cannot unilaterally eliminate dark patterns. However, by working closely with UX and marketing departments, privacy teams can help reduce the presence of these patterns.

UX

UX professionals have valuable insights into an enterprise's users. They ensure user friendliness in design and serve as user advocates.

Privacy professionals often work closely with information security, legal and compliance and risk management teams, but only one-third of privacy professionals always or frequently work with product/business

development teams.²⁰ Privacy professionals and UX professionals both need to think about the user: privacy teams consider the privacy perspective, while UX teams consider the user's experience. Together, they can optimize the user's journey in a privacy-centric way. Additionally, the UX team can help ensure that privacy is not traded for functionality or vice versa.

Marketing

Marketing professionals often want a lot of information about existing and potential customers. This can help them target advertising content to individuals who may be more likely to act on it. But it is possible to gain this insight without deceiving people into giving up their information. **Figure 10** shows an email preference box that allows users to indicate what kind of communication they would like to receive. In addition to allowing users to clearly indicate their preferences, this method may also increase engagement as users self-identify their interests rather than marketers assuming interests based on tracking.

²⁰ ISACA, Privacy in Practice 2023, 2023, <https://www.isaca.org/resources/reports/privacy-in-practice-2023-report>

FIGURE 10: Opting Into Marketing Emails

Please let us know what emails you'd like to receive from us:

☐ All marketing emails

☐ All sales emails

☐ New product releases

☐ Unsubscribe from all emails

Privacy professionals should stress to marketing teams that tricking people to get consent for tracking, intentionally or not, will likely backfire.

Privacy professionals must also educate those in marketing on the harm manipulative copy can cause and why it constitutes a deceptive pattern in the eyes of consumers. Any temporary revenue gains from deceiving people into providing personal data will likely be outweighed by the long-term loss of trust with consumers. Emphasize that meeting compliance requirements is the bare minimum, and gaining trust may require going above and beyond what compliance mandates.

Simplifying the User's Privacy Experience

UX refers to the method of creating products for users in a useful way.²¹ UX's focus on the user makes it complementary to privacy by design, where privacy engineering should be user centric. An enterprise's UX department has a lot of insight into users, which can greatly shape how privacy information is conveyed and privacy settings are presented.

UX professionals empathize with users, which privacy professionals should also do. Operating as an advocate for users can ensure that business practices and interface design are user friendly. Working alongside UX professionals, privacy professionals may need to argue for practices and principles that seem at odds with some business desires. And although compromises may need to occur, privacy professionals can ensure that their enterprise defaults to protecting privacy.

Any temporary revenue gains from deceiving people into providing personal data will likely be outweighed by the long-term loss of trust with consumers.

Given that 53 percent of technical privacy professionals describe their enterprises as somewhat or significantly understaffed,²² it is not feasible to expect privacy professionals to lend their expertise to every development project.

Nonetheless, privacy professionals can teach development and UX teams about privacy to help ensure that it is a consideration in the design of future projects.

21 Interactive Design Foundation, "User Experience (UX) Design," <https://www.interaction-design.org/literature/topics/ux-design>

22 Op cit ISACA

The following are a few points for privacy professionals to emphasize to UX designers:

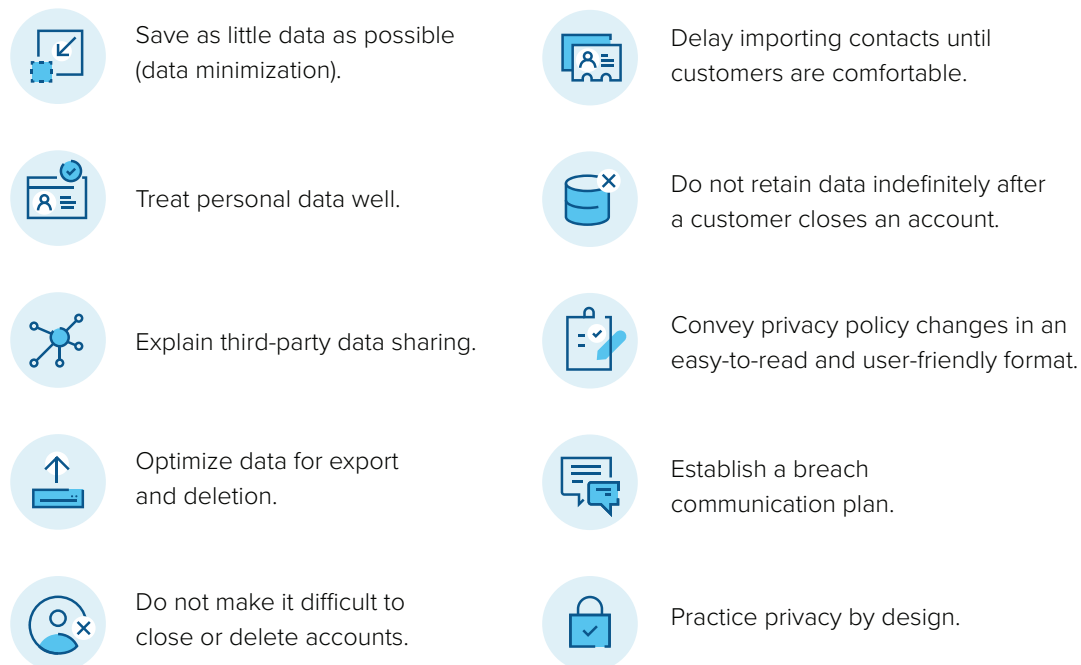
- Expressing a desire not to be tracked should take the same number of clicks as consenting to tracking.
- The default setting should be that the least amount of information necessary is collected.
- Users should not have to take any action to have their privacy protected.
- Tricking people into giving their consent can have costly ramifications.
- Some information is considered personal information, and certain conclusions can be drawn from information collected by the

enterprise (e.g., how location data could reveal a person's medical conditions).

- There may be privacy compliance concerns and pending privacy-related legal actions.

UX designers may be familiar with the Privacy-Aware Design Framework, a set of guidelines that help facilitate design with privacy in mind. **Figure 11** shows the Privacy-Aware Design Framework guidelines.²³ This framework can serve as the starting point for a conversation between privacy teams and UX designers.

FIGURE 11: Privacy-Aware Design Framework



Deceptive Patterns at Small-to-Medium Enterprises

Smaller or newer enterprises may not have UX personnel on staff, or the UX designers may not have the bandwidth to collaborate with privacy teams. In this case, privacy professionals who want to advocate for user experience can find guidelines on good design in the Web Content Accessibility Guidelines (WCAG).²⁴ The WCAG give guidance on how to ensure content is available to people with a variety of accessibility needs and remove deceptive patterns that result from poor visual design (e.g., hard-to-read toggles or lack of contrast).

Privacy professionals at smaller enterprises may be at an advantage over those at larger ones because there are fewer departments that create consumer-facing content and resources. At many large enterprises, privacy professionals are not capable of meeting with someone from every part of the enterprise that collects data and ensuring they do not use dark patterns. In contrast, privacy professionals at smaller enterprises can have more insight into the data various departments—such as marketing, human resources and finance—collect and use.

²³ Friedman, V.; "Privacy UX: Privacy-Aware Design Framework," *Smashing Magazine*, 25 April 2019, <https://www.smashingmagazine.com/2019/04/privacy-ux-aware-design-framework/>

²⁴ Web Content Accessibility Guidelines, "Designing for Accessibility," <https://wcag.com/designers/>

Privacy professionals should consider the users who will need to modify their privacy settings. Given limited resources, designing for every potential data subject might not be possible. For this reason, it is useful to design for a new

consumer, i.e., someone unfamiliar with the enterprise and its application or website settings. Odds are, if privacy settings are designed with a new user in mind, experienced users will also be able to navigate them.

Putting This Into Practice

Ideally, an enterprise will eliminate all dark patterns. But UX and privacy teams will likely experience some pushback when encouraging other departments to rein in deceptive patterns. Many business models inadvertently rely on deceptive tactics for collecting and processing information. Privacy professionals should not compromise on advocating for data subjects. Enterprise leadership may make decisions that are antithetical to privacy rights, but privacy professionals have the responsibility of making the business aware of deceptive patterns and the impact they can have.

When advocating for eliminating dark patterns, it may be helpful to cite laws and enforcement actions related to them; this can help quantify the monetary consequences of failing to address dark patterns. This can be done as part of a privacy impact assessment or data protection impact assessment, which may be an enterprise requirement depending on the jurisdiction.²⁵ Explain the reputational harm that comes from employing dark patterns. Listen to the concerns of departments that rely on deceptive patterns and explore if there may be a way for them to collect the information they need without tricking data subjects.

Conclusion

Many enterprises rely heavily on privacy dark patterns to track customers, but those that proactively address dark patterns and adhere to consumers' privacy preferences can gain a competitive advantage. Privacy professionals alone cannot eliminate an enterprise's dark patterns; they must work closely with other departments that create consumer-facing products, services, websites and content. Privacy professionals should note the deceptive

patterns they encounter in their personal lives and ensure their enterprise does not employ them as well. Working to remedy design that forces users to give up their privacy can help build digital trust with consumers, leading to numerous benefits, including a positive reputation, more reliable data for decision-making and fewer privacy breaches and cybersecurity incidents.²⁶

25 GDPR.EU, "Data Protection Impact Assessment (DPIA)," [https://gdpr.eu/data-protection-impact-assessment-template/#~:text=A%20Data%20Protection%20Impact%20Assessment%20\(DPIA\)%20is%20required%20under%20the,help%20you%20execute%20the%20assessment](https://gdpr.eu/data-protection-impact-assessment-template/#~:text=A%20Data%20Protection%20Impact%20Assessment%20(DPIA)%20is%20required%20under%20the,help%20you%20execute%20the%20assessment)

26 ISACA, State of Digital Trust 2023, 2023, <https://www.isaca.org/digital-trust/state-of-digital-trust>

Acknowledgments

ISACA would like to recognize:

Expert Reviewers

Yunique Demann

CISA, CISM, CDPSE, CCISO, CIPT, CISSP
USA

Kevin Fumai

CDPSE, CIPP/US/E, CIPM, CIPT, FIP, PLS, CCSK, CEET
USA

Larisa Gabudeanu

CISA, CISM, CRISC, CDPSE
University Babes-Bolyai, Romania

Mathew Holdt

CISA, CIA, CFE
Protiviti, USA

Ng Wai Hou

CDPSE
Macau

Roy Marra

CRISC, CDPSE
IESO, Canada

Peter Matavovszky

CISM
Switzerland

Ryan W. McCuskey

McCuskey LLP
USA

Nandita Rao Narla

CISA, CISM, CRISC, CDPSE, CIPM, CIPP/US, CIPT, FIP
USA

Kane Porter

CISA, CIPP/C
Canada

Juan Pablo Barriga Sapiencia

CSX-P, CDPSE, CompTIA (A+, Network+, Security+) LPIC-1
Bolivia

Board of Directors

John De Santis, Chair

Former Chairman and Chief Executive Officer, HyTrust, Inc., USA

Brennan P. Baybeck, Vice-Chair

CISA, CISM, CRISC, CISSP
Senior Vice President and Chief Information Security Officer for Customer Services, Oracle Corporation, USA

Stephen Gilfus

Managing Director, Oversight Ventures LLC, Chairman, Gilfus Education Group and Founder, Blackboard Inc., USA

Niel Harper

CISA, CRISC, CDPSE, CISSP, NACD.DC
Chief Information Security Officer, Data Privacy Officer, Doodle GmbH, France

Gabriela Hernandez-Cardoso

NACD.DC
Independent Board Member, Mexico

Jason Lau

CISA, CISM, CGEIT, CRISC, CDPSE, CIPM, CIPP/E, CIPT, CISSP, FIP, HCISPP
Chief Information Security Officer, Crypto.com, Singapore

Massimo Migliuolo

Independent Director, Former Chief Executive Officer and Executive Director, VADS Berhad Telekom, Malaysia

Maureen O'Connell

NACD.DC
Board Chair, Acacia Research (NASDAQ), Former Chief Financial Officer and Chief Administration Officer, Scholastic, Inc., USA

Asaf Weisberg

CISA, CISM, CGEIT, CRISC, CDPSE, CSX-P
Chief Executive Officer, introSight Ltd., Israel

Erik Prusch

Chief Executive Officer, ISACA, USA

Pamela Nigro

ISACA Board Chair 2022-2023
CISA, CGEIT, CRISC, CDPSE, CRMA
Vice President, Security, Medecision, USA

Gregory Touhill

ISACA Board Chair 2021-2022
CISM, CISSP
Director, CERT Center, Carnegie Mellon University, USA

Tracey Dedrick

ISACA Board Chair, 2020-2021
Former Chief Risk Officer, Hudson City Bancorp, USA

About ISACA

ISACA® (<https://www.isaca.org/>) is a global community advancing individuals and organizations in their pursuit of digital trust. For more than 50 years, ISACA has equipped individuals and enterprises with the knowledge, credentials, education, training and community to progress their careers, transform their organizations, and build a more trusted and ethical digital world. ISACA is a global professional association and learning organization that leverages the expertise of its 170,000 members who work in digital trust fields such as information security, governance, assurance, risk, privacy and quality. It has a presence in 188 countries, including 225 chapters worldwide. Through its foundation One In Tech, ISACA supports IT education and career pathways for underresourced and underrepresented populations.

DISCLAIMER

ISACA has designed and created *Eliminating Deceptive Privacy Practices: Building Trust by Addressing Privacy Dark Patterns* (the “Work”) primarily as an educational resource for professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

RESERVATION OF RIGHTS

© 2023 ISACA. All rights reserved.



1700 E. Golf Road, Suite 400
Schaumburg, IL 60173, USA

Phone: +1.847.660.5505

Fax: +1.847.253.1755

Support: support.isaca.org

Website: www.isaca.org

Provide

Feedback: www.isaca.org/eliminating-deceptive-privacy-practices

Participate in the ISACA Online

Forums:

<https://engage.isaca.org/onlineforums>

Twitter:

www.twitter.com/ISACANews

LinkedIn:

www.linkedin.com/company/isaca

Facebook:

www.facebook.com/ISACAGlobal

Instagram:

www.instagram.com/isacanews/