cgl

THE PRIVACY HANDBOOK

5 Trends to Watch in 2024 & Beyond

TABLE OF CONTENTS

Introduction

Privacy has been one of the most dynamic areas of law over the past five years. New laws are coming uncharacteristically quickly, leaving companies struggling to keep up. In this resource, we contemplate some trends we're expecting to see in 2024, then outline some key practices that can help companies future-proof their operations against anticipated changes and ongoing challenges.

We are CGL LLP, a fully distributed transactional law firm focused on providing quality services to our clients and great work-life balance to our attorneys.

Hannah Genton and Noam Cohen,
Founding Partners at CGL.

1 TREND: Compliance Challenges Will Become More Complex

2023 brought a host of changes to the privacy landscape in the US: Additional privacy obligations came into effect in California, and comprehensive consumer privacy laws in Virginia, Colorado, and Connecticut also entered into force. Utah's comprehensive data privacy law will commence on December 31, 2023, closing out the year.

2024 will see a wave of additional privacy laws across the US, including new laws in Florida, Oregon, and Montana. Businesses will also need to begin preparing for laws that have passed in their respective state legislatures but won't come into effect until 2025-2026. This includes comprehensive privacy laws in Texas, Tennessee, Iowa, Indiana, and Delaware.

Broadly, these laws all contain the following rights:

- Right to access;
- Right to delete (though the scope of this right can vary from one state to another);
- Right to opt out of processing for profiling or targeted advertising purposes (except Iowa);
- Right to portability;
- Right to opt out of sales;
- Right to opt-in for sensitive data processing (except Iowa);
- Right to opt out of certain automated decision-making;
- Risk assessment requirement (except Iowa);
- Privacy notice requirement; and
- Purpose limitations.

Some Key Differences in the 2023 US State Privacy Laws

- Indiana's and Iowa's privacy laws do not include any revenue thresholds, like other US states. Instead, application of the law is based on the volume of personal data a business controls and processes (more than 100,000 consumers) or the volume of personal data processed (more than 25,000 consumers) where 50% of gross revenue is derived from that data.

- Businesses in Texas are covered by the law if they (1) operate in Texas or target Texas residents, and (2) process or engage in the sale of personal information, and (3) are not excluded as a small business. This is a different standard from other states.

- Transgender or nonbinary status is included in Oregon's and Delaware's definition of sensitive data. Delaware's definition of sensitive data also includes pregnancy.

Many other states are contemplating their own comprehensive consumer privacy laws and we expect this momentum to continue in 2024. Maine, Massachusetts, New Hampshire, New Jersey, North Carolina, Pennsylvania, and Wisconsin all (at the time of writing) have bills moving through their lawmaking processes. That's not to say these states will all pass the laws in 2024, however. We expect some to pass and some to be blocked along the way.

There's also a possibility that we will see a federal privacy law in 2024 – though we would be surprised to see that come to pass.

2 TREND: We'll Continue to See Huge Fines in the US

Regulatory fines have been escalating in the last few years – often setting new records. Huge fines have been particularly common for violations of children's privacy. These are some of the recent Children's Online Privacy Protection Act (COPPA) penalties we've seen the U.S. Federal Trade Commission (FTC) hand out to businesses:

MICROSOFT'S COPPA SETTLEMENT – $20 MILLION

Microsoft agreed to pay $20 million to settle charges that it violated the COPPA when it collected children's data without parental consent and retained that data. It is also required to boost its children's privacy practices.

The claim arose from Microsoft's poor privacy practices relating to its Xbox gaming system. Microsoft's sign-up process asked users to provide their email address, name, date of birth and, prior to late 2021, their phone number. Despite some users indicating that they were children under 13, Microsoft collected and retained this information without requesting parental consent.

Under the settlement order, Microsoft is also required to:

- Provide additional notices to parents who have not created a separate account for their child, informing them that doing so will provide privacy protections for their child by default;
- Obtain parental consent for accounts created before May 2021 (where the user is still under 13 today);
- Establish and implement compliant data retention and deletion processes for children's data; and
- Implement systems that notify publishers when disclosed information relates to a child and that require publishers to apply COPPA protections.

Interestingly, the order also clarifies that avatars generated from a child's image are considered personal information and fall under the COPPA.

AMAZON'S COPPA SETTLEMENT – $25 MILLION

Amazon was accused of 'prominently and repeatedly' assuring users that voice recordings collected through the Alexa voice assistant and geolocation information collected through the app could be deleted. However, Amazon retained the information for years to use it to improve its Alexa algorithm.

This was a COPPA issue because Amazon collected voice recordings from children and stored them indefinitely. When parents asked Amazon to delete the information, it kept transcripts of what kids said.

In addition to the $25 million penalty, Amazon was required to delete the data and inactive children's Alexa accounts. It must also implement significant changes to its privacy notices and data retention and deletion processes.

EPIC'S COPPA SETTLEMENT – $275 MILLION (THE LARGEST TO DATE)

The FTC settled its claim against Epic Games, Inc – the company behind the immensely popular video game Fortnite – for $520 million. This was comprised of $275 million for COPPA violations and $245 million in refunds for customers who were tricked (through **deceptive dark patterns**) into making purchases. Each of these settlements was for a record-breaking sum.

Regarding the COPPA violations, the FTC alleged that Epic:

- Collected personal information from children under 13 without notifying their parents or obtaining their parents' verifiable consent; and
- Enabled real-time voice and text chat communications for children and teens by default, in violation of the prohibition against unfair practices.

In addition to the financial penalty, Epic must also:

- Delete previously collected personal data for children under 13 unless their parents provide affirmative consent for Epic to keep it; and
- Establish and implement a privacy program that addresses the issues identified by the FTC. This program will be subject to regular independent audits.

PENALTIES FOR DECEPTIVE DARK PATTERNS

There was also a spate of FTC orders in Q1 2023 about deceptive dark patterns, including the following:

- Credit services company, Credit Karma, was fined $3 million for using dark patterns to misrepresent "pre-approval" for credit cards to consumers (**January 2023**).

- Telehealth and discount prescription drug provider, GoodRx, was ordered not to use dark patterns when obtaining users' consent to share sensitive health data with advertisers. GoodRx will also have to pay a $1.5 million penalty (**February 2023**).

- Epic Games, was ordered to refund $245 million to consumers, part of which will go to users who were tricked into making purchases while playing the game, Fortnite, through the use of dark patterns (**March 2023**). In June, the FTC commenced proceedings, alleging Amazon used dark patterns to enroll users in Amazon Prime without consent. The Commission also settled a suit against Publishers Clearinghouse in the same month, alleging that the company used dark patterns to deceive users about the terms of its well-known sweepstakes.

While these cases focused on deceptive subscription practices, they, nevertheless, show us that the FTC continues to view dark patterns as an enforcement priority. We expect to see additional enforcement actions in this sphere through 2024.

3 TREND: Attitudes Towards Privacy Will Shift

As privacy laws continue to develop around the country (and the world), we're seeing an increase in the number of companies looking to 'privacy-proof' their operations. This is a shift from the more checklist compliance approach we've seen dominate the privacy landscape in past decades.

THE BENEFITS OF PRIORITIZING PRIVACY OVER COMPLIANCE

Trust is arguably the currency of the modern digital age. We live in a world where data breaches dominate the headlines, and customer loyalty is fickle. It is widely accepted that taking privacy seriously can give businesses a legitimate competitive advantage that has the added benefit of safeguarding your reputation and minimizing your legal risk.

We're also seeing an increasing number of organizations leveraging privacy as an opportunity for innovation. The drive to avoid intrusive and/or excessive data collection practices prompts companies to think outside the box to find practices that resonate positively with customers. These changes can be as simple as not requesting credit card details from potential leads who want a free trial.

In practice, privacy-first companies tend to prioritize most or all of the following:

- **Data minimization**;
- **Privacy by Design**; and
- **Regular audits and assessment**

This doesn't mean other compliance obligations, like clear consents, transparency, and user controls don't matter. But prioritizing "big picture" tasks, like limiting the amount of data you collect, building privacy in from the beginning, and identifying privacy risks early can make those other compliance burdens lighter.

A Case for Compliance-First

Compliance is not avoidable. While it's challenging (seemingly impossible sometimes) for companies to become fully compliant with all privacy laws, it's not advisable to throw compliance and the associated checklists to the wayside.

A compliance-first approach, while reactive, may have some cost savings over a privacy-first approach – especially in the short term. Compliance can also help you benchmark where your processes are working and where you can make improvements. Finally, compliance is what you will be judged on if you do ever face a complaint or investigation.

Beyond the Legal Labyrinth

Ultimately, however, a privacy-first approach wins when it comes to agility and the desire to develop a more 'future-proof' privacy program.

Regulations, though crucial, lag behind technological advancements and changing consumer expectations. By aligning operational strategies on privacy, businesses are able to be proactive, rather than reactive, in this shifting landscape. They are better positioned to 'guess' what future regulation will look like and develop cost-effective and sustainable strategies that stand the test of time. They're also better positioned to adapt swiftly to emerging challenges and seize new opportunities.

Shifting Attitudes Towards Data Collection

We're also seeing a change in attitude towards data collection and retention.

Data collection is a ubiquitous practice in modern business, with companies collecting personal information to deliver products and services, engage in targeted marketing, and offer personalized customer service (among many other things). At the same time, consumers have become painfully aware of the risks that come with trusting businesses with their data. Someone suffers identity theft every 22 seconds, **according to identitytheft.org**, with the average cost being $500.

Practicing data minimization is a crucial tool in reducing the risk to consumers who provide information to your business. It also reduces risk to your business by limiting your exposure to fines and reputational damages if things go wrong. So, let's delve into what data minimization looks like in practice.

Data Overcollection Comes with Significant Risks

Beyond the many costs associated with a data breach, data overcollection may also lead to decreased consumer trust. Several factors drive this – and any one factor can negatively impact consumer trust, reduce loyalty, and drive down sales. Some of the drivers are that consumers:

- Worry their identity may be stolen;
- See your business as greedy – caring more about scooping up data (and the potential profit that comes from it) than consumer safety;
- Feel that your business isn't being transparent; or
- Perceive a loss of control over their data.

Where Data Overcollection Went Wrong

The risks associated with data overcollection aren't just hypotheticals put forward by risk-averse lawyers. There are countless real-world examples of data overcollection resulting in real consequences.

- **The Cambridge Analytica scandal** is the highest-profile example.
- The Marriot data breach in 2018 resulted in a $23 million fine and a **5.6% decrease in its premarket stock price**. The hackers exfiltrated information about hundreds of millions of guests, including credit card information and unencrypted passport information.
- The **Flo Period app penalty and the recent FTC penalty against GoodRx** are examples of where companies collect data and then sell it to advertising companies without disclosing this use to consumers.

In response to the risk, we're seeing an increase in the number of companies adopting a 'less is more' approach to data collection. And we expect to see this trend gain traction in 2024.

4 TREND:
Privacy-Enhancing Technologies Will Become More Available

Privacy-Enhancing Technologies (PETs) are currently in their infancy, but they hold the potential to bring a seismic shift in data management. In an era where data forms the linchpin of many business models, PETs stand out as harbingers of more respectful and safe data aggregation and analyses.

"By 2030, data marketplaces enabled by PETS, in which individuals, corporate machines and governments trade data securely, will be the second largest ICT market after the Cloud." – Lunar Ventures report ***The privacy infrastructure of tomorrow is being built today***.

The OECD currently defines PETs "as a collection of digital technologies, approaches and tools that permit data processing and analysis while protecting the confidentiality, and in some cases also the integrity and availability, of the data and thus the privacy of data subjects and commercial interests of data controllers".

It goes on to outline that these technologies, tools, and approaches generally fall into four categories:

1. Data obfuscation;
2. Encrypted data processing tools;
3. Federated and distributed analytics; and
4. Data accountability.

Use Cases for PETs

Verification of Sensitive Personal Information

Zero-Knowledge Proof (ZPK) tools can eliminate the need for people to submit sensitive personal information for routine purposes. For instance, these tools would allow renters to prove to realtors that they have an income over a certain amount without showing specific sensitive financial information.

These tools are not yet mature. But they are seen as a key element in the future of projects like the **Digital Identity Wallets** Europe plans to implement. And it's expected that their applications and use will widely expand in the near term.

Product Development and Improvement

Apple highlighted how personal information and product development are intertwined:

"There are situations where Apple can improve the user experience by getting insight from what many of our users are doing, for example: What new words are trending and might make the most relevant suggestions? What websites have problems that could affect battery life? Which emoji are chosen most often? The challenge is that the data which could drive the answers to those questions—such as what the users type on their keyboards—is personal." - Apple's Differential Privacy Overview.

It then went on to discuss how differential privacy is already being used to solve issues like these. Generally, differential privacy is a technique that adds 'noise' to a dataset to protect individual privacy while allowing for statistical analysis. Apple has already widely adopted differential privacy to improve privacy during **photo analysis** and to gain insights about the **use and usability of certain functions**.

More Privacy-Centric Targeted Digital Advertising

*"We hope that in the future PETs will allow a person's original piece of data to be anonymized and aggregated with other people's information. This new piece of data can then be leveraged by [Meta] and allow advertisers to continue running and measuring personalized ads." – **Meta**.*

PETs can help advertisers reach their audience without directly accessing individual user data. The implications of this would be huge in the targeted advertising space, since it promotes compliance with privacy regulations and user consent – and improves privacy outcomes for individuals. Some examples of PETs that could apply to the digital advertising ecosystem include differential privacy, federated learning, and homomorphic encryption, which allow for data processing without revealing individual data points.

Heathcare and BioTech Data Analysis

PETs offer significant potential in the healthcare and biotech industries. A 2022 blog post about the potential benefits of PETs imagined a future where:

- Tools are being developed for physicians to identify early signs of cancer and reduce health disparities without accessing anyone's private data; and
- Cities and states can rapidly share public health data without sharing personal information about individuals.

Source: The White House

What Should Companies Do Now?

As we outlined, many of these technologies are in their infancy and their adoption and use is not (yet) widespread.

For now, we would suggest creating and keeping a catalogue of your biggest privacy challenges. Then, identify situations where the choice seems to be either consumer privacy or company benefit. These are the scenarios where PETs will likely play a role in the coming years.

5 TREND: Privacy UX Will Become the Norm

You've likely seen a call to action somewhere online designed to get you to choose the less privacy-centric (or more data-intrusive) option:

- A pop-up window with two buttons: one saying "Subscribe to save 10%" (which requires you to provide your email address) and the other saying "No, I don't like discounts".
- An unsubscribe button with the note "Ten kittens will cry if you [Unsubscribe]".
- A "Get it free" button, which transports you to a page asking for your credit card details (and, in some cases, your social security number).

This is 'Dark UX' in practice.

First Things First: What is UX?

UX, or **"User Experience"**, refers to the ease with which a person interacts with a product, system, or service. Apple products are known for their extremely good UX – meaning most end-users of Apple's products find them easy and enjoyable to use.

> ***Privacy UX delves deeper into the user experience by emphasizing transparent and user-friendly interactions related to a user's personal data.***
> ***It seeks to ensure that users not only understand and easily control how their data is used but also trust the entities handling their information.***

Dark UX, on the other hand, refers to design strategies that prioritize business goals at the expense of the user's best interests. These strategies can often mislead, confuse, or manipulate users into taking actions they might not have taken otherwise.
"Dark Patterns" are a part of Dark UX. They are deceptive design tricks that intentionally guide users toward decisions that benefit the business, usually at the user's expense.

For instance, a dark pattern might make it very easy to sign up for a recurring charge but convoluted and/or time-consuming to cancel that same charge.
(**The Federal Trade Commission has warned businesses against this practice.**)

For clarity: Dark UX and Dark Patterns are intertwined in that the former often employs the latter to achieve its goals (manipulating the user).

Why Does Dark UX Exist?

Dark UX (and the use of Dark Patterns) can lead to short-term gains for businesses. They have been shown to increase subscriptions and revenue in the short term. However, employing them is short-sighted because they also erode trust, damage brand reputation, and lead to user frustration in the long term.

Moreover, as users become more aware and regulatory bodies clamp down, businesses might find themselves facing backlash or legal consequences for such designs. We're already seeing the **FTC hand out significant penalties for the use of dark patterns**.

IMPLEMENTING PRIVACY UX

The bottom line is privacy-centric UX is an easy and relatively cheap way to reduce the risk introduced by the slate of new privacy laws coming into effect across the US and worldwide.

It's also an easy and relatively cheap way to build trust, promote loyalty, and avoid the negative impacts of Dark UX.

TAKEAWAY FOR READERS:

Future-Proof Privacy Best Practices Checklist

Implementing these practices can help future-proof your privacy practices and align with the trends we're expecting to see throughout 2024 – and beyond:

Prioritize Simplicity and Clarity

Clear, Simple Language

The language you choose to share privacy-related information is going to be critical to user understanding. You should prioritize clear, simple language that is devoid of jargon when explaining privacy settings and options.

Easy Access to Privacy and Account-Level Controls

Users should be able to easily access and change their privacy settings and account details, including the option to close their account and/or delete their data.

Immediate Feedback

If a user changes a privacy setting, you should offer immediate feedback showing that the change has been made (where possible).

Document and Review the Data You Collect

You should identify and document the types of personal data and sensitive information you collect. It's essential that you know and understand what data you collect and why.

From there, you should evaluate whether it is truly necessary to collect and store these types of data. An essential part of this is considering whether there are alternatives to collecting and storing it. For instance, you may not need to collect a physical address, email address, and phone number to facilitate a delivery. Perhaps just two of those categories will suffice. Resist the temptation to collect (and keep) data that might be useful down the road. You can't lose what you don't have.

Then, implement data retention policies to ensure you keep data only as long as you need it. You should judge this based on the reason you initially collected the data, not potential future uses for it.

Finally, regularly review your data collection policies and practices. It's a good practice to audit your data collection practices routinely, but the following events should also act as a prompt:

- Any change in the law;
- A data breach;
- Significant changes to your operations;
- Mergers or acquisitions; and
- An increase in customer complaints or requests to access or delete their data.

Introduce More Intrusive Privacy Settings at the Right Time

This is something we see mobile development get wrong all the time. Most mobile apps seek extremely privacy-intrusive permissions from the outset (access to contacts, the camera and microphone, and location are common culprits). This is a turn off for many users.

Privacy UX, on the other hand, would introduce these settings (and ask for consent to collect the data) when (and only if) the user wants to access functionality those settings impact.

Let's look at an example of a flashlight app asking for access to your location when you download the app. Would you download the app – or would you not trust it because of the intrusive privacy settings?

What about if you later found out that it had (optional) functionality that would automatically turn off the flashlight after five minutes during daylight hours to prevent the battery draining if it were accidentally turned on? It would need access to your location (and time zone) to complete this task, and it asks for permission (and explains why it's needed) when you turn on this functionality. That's much better, right?

If You Operate a Child-Directed Website:

It is critical that you obtain verifiable consent from parents before collecting personal information from children under 13 – consider asking for age at the outset so you know right away whether you need to collect parental consent or not. You should also:

- Collect verifiable parental consent before generating avatars for children.
- Make sure you're providing notice to parents about what types of information you are collecting and be aware that this generally requires two forms of notice – an online notice and a direct notice to parents.
- Establish and maintain robust data deletion processes to ensure you delete children's data within a reasonable period.

Do You Need Help Navigating Privacy in 2024?

Our experienced privacy attorneys would love to help.

Let's Talk

Let's Talk

cgl