Are Organizations Ready for New Privacy Regulations?

Based on 1,200 privacy statements, many are not prepared for coming regulations.

Online Trust Alliance
an **Internet Society** initiative

www.internetsociety.org/privacystatements

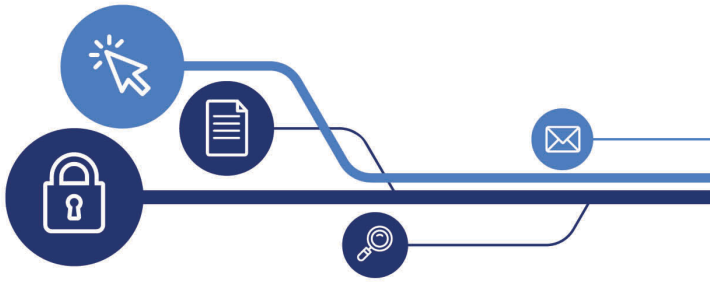
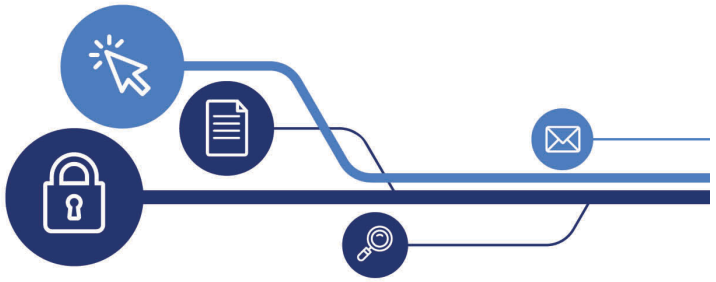


Table of Contents



Scope

The 10th Online Trust Audit[1] by the Internet Society's Online Trust Alliance (OTA) analyzed 29 variables in 1,200 privacy statements to determine how well they convey information to users. In this report, we take another look at these privacy statements in the context of common themes across three global privacy regulations.

It would be virtually impossible to cover every new privacy regulation around the world. We will focus on three established ones:

1. **General Data Protection Regulation (GDPR)**[2] in the European Union that went into effect in May 2018.
2. **California Consumer Privacy Act (CCPA)**[3] in the United States that goes into effect 1 January 2020.
3. **Personal Information Protection and Electronic Documents Act (PIPEDA)**[4] in Canada that went into effect in April 2000.

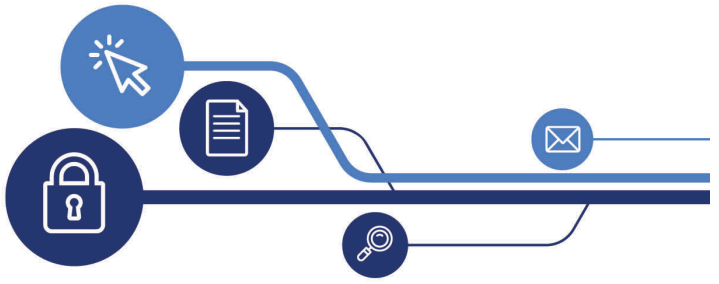
Why Are Privacy Statements Important?

Privacy statements are only one part of an organization's overall privacy stance, but it is the first point at which users are informed about its policies. Privacy statements are an agreement between the organization and the user. If that statement is incomplete or hard to understand, it opens the organization to regulatory fines and leaves users without a full understanding of how the organization handles their data.

The privacy regulations covered here differ in how they handle communication with users, but they have common threads that ensure users are informed about their rights and informed about what organizations are doing with their data. OTA's guidelines include similar provisions regarding how privacy statements can best be structured for readability, what information organizations should include, and other criteria to ensure users are as informed as possible.

It is worth noting that most of the 1,200 organizations evaluated in the Online Trust Audit are based in the United States and are therefore not legally obligated to fulfil the requirements of any of these privacy regulations. Nonetheless, they give us an important look at how organizations of all sizes and in all industry sectors may be preparing for new privacy regulations.

1 https://www.internetsociety.org/resources/ota/2019/2018-online-trust-audit-and-honor-roll/
2 https://eugdpr.org/
3 https://www.caprivacy.org/
4 https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/



OTA's Privacy Guidelines Mapped to Global Privacy Regulations

GDPR, CCPA, and PIPEDA, and indeed many other privacy regulations around the world, share common principles that are measured in OTA's Online Trust Audit. The principles that map to specific provisions of the Audit's criteria include:

1) Users must be able to request information on why their personal information is being collected.
2) Users must be informed if their personal information will be sold or shared with a third party.
3) Users must have access to their data, and be able to download it, and it must be "portable" (i.e. in an easily readable format).
4) Users must be able to request their data be deleted.
5) Organizations must notify users of their rights in an easily understandable matter.

This list is not exhaustive regarding what these regulations cover in terms of data privacy, but they are criteria we can measure using Audit data to shed some light on how our sample of organizations is doing given privacy regulations around the world.

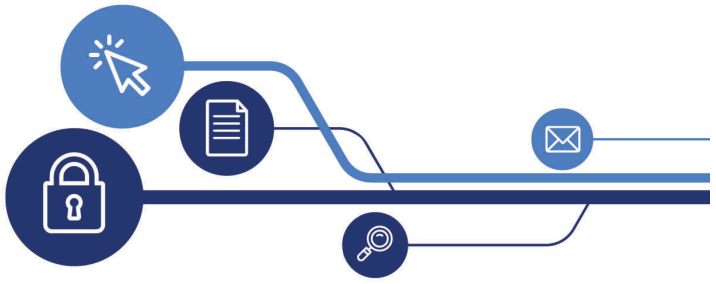
Users Need to Know How Their Data is Handled

Data sharing language. In our Audit, the vast majority (98%) of privacy statements had some language about data sharing. In addition, two-thirds (67%) included a statement that the company does not sell or share data with third parties. Both of these types of statements are required in many privacy regulations around the world, where data sharing is often the largest element addressed.

Notifying users when data is shared. We did not see language saying that users must be *notified* when their personal data is sold or shared. While this is common in newer privacy regulations, our Audit data on privacy statements was collected in early 2019 and almost entirely from U.S.-based organizations, none of whom would have been required to do this at the time.

Holding third parties to same standards. In a similar vein, many privacy regulations say that organizations must ensure that third parties they work with are held to the same data sharing standards they hold themselves to. We measure this in the Audit, and 57% of organizations said they hold third parties to this standard.

Disclosing types of third parties shared with. In addition, these regulations state that organizations should also disclose the *types* of third parties data could be potentially shared with. For example, if data is shared with payment vendors the statement must disclose that. Less than 1% of companies in the Audit had language outlining the types of third parties in this way. These laws rarely require the organization to list actual partners, simply that users are informed about the kinds of third parties their data could be shared with.



Social media data collection. A similar concept is disclosing to users if the organization uses social media sites that might also be collecting user data – 52% of statements informed users that the site used third party social media services.

The issue of vendors and social media sites is also important for security reasons. Many unauthorized data releases occur when an attacker accesses an organization's data through a third party. A recent example was the breach of American Medical Collections Agency (AMCA), a collections agency for medical labs such as Quest Diagnostics and LabCorp, which affected more than 20 million users.[5]

Data retention. Many privacy regulations have added data retention as an important concept. This is largely because data that is stolen or released is often old and the organization did not need to keep it. Overall, few organizations in our Audit had explicit language about data retention (2%), but as laws evolve they will have to take this concept more seriously since many countries around the world are including this in their privacy laws.

Reason for data collection. Related to data sharing, a major feature of all of these privacy regulations is that users need to be informed *why* their data is being collected. Of the organizations assessed in the Audit, 95% had some language explaining why they are collecting user data.

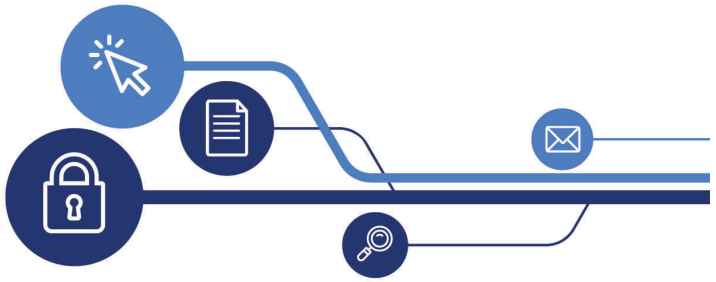
Cross-device tracking. A similar concept in OTA's scoring is that statements should explicitly tell users if the site is collecting data to track them across devices – 47% of statements included such language. While this is not called out expressly in many privacy regulations, it fits the theme that users need to know *why* data is being collected. If an organization is collecting user data in order to track the user across devices, sometimes referred to as "fingerprinting," all of these new regulations would require the organization to disclose that fact.

Integration of outside third-party data. Finally, organizations should also disclose if they use third-party data about users for their services. Almost half of organizations (43%) had such a disclosure. Similar to social media disclosures, users need to be aware that organizations they are interacting with are most likely using data about them from third parties and that data may be used in conjunction with data collected by the organization itself.

Users Need a Clear Way to Contact Organizations About Their Data

Contact information. Because it is a requirement in these regulations that users must have access to their data in some fashion, the first clear step is that organizations must have a way for users to contact them. In the Audit, 70% of organizations had a clear contact, though it ranged from an actual Data Protection Officer (DPO) to a generic contact email address.

5 https://www.zdnet.com/article/amca-data-breach-has-now-gone-over-the-20-million-mark/



OTA's bar for this requirement was fairly low, requiring only the presence of an email address. This is not true, however, of all three of the regulations discussed here and of many others. Going forward, organizations will be required not only to identify a specific person or department that handles data protection, but must inform users how to contact that specific department directly.

State how to request data. Organizations must clearly state what data users can request – 50% of organizations had some language outlining user rights. However, for the purposes of the Audit the bar for this language was also low. Organizations only had to have some language indicating users had the ability to contact them. Hardly any in the Audit adhered to the much stricter standard laid out in the principles above to outline exactly what data the user could ask for and how to do it, let alone delete it. This, again, is likely due to the fact that this data was collected in early 2019 and included primarily U.S.-based organizations, none of which would have been directly held to this higher standard. This will change, however, when the CCPA goes into effect in 2020. Even U.S. companies will have to be much more transparent about user access to their data if they do business in California.

Statements Need to be Understandable

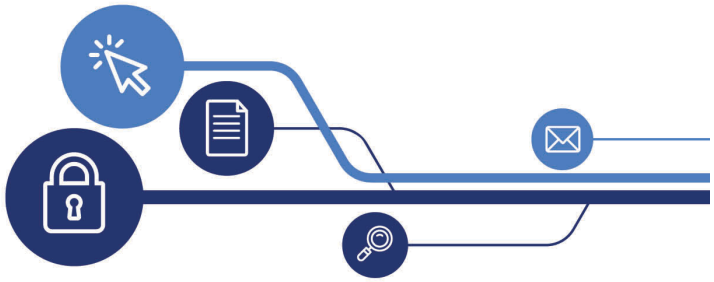
OTA also advocates several practices that help privacy statements be "readable," a concept advocated by many privacy regulations. The details for readability vary across laws and cultures (after all, the concept of "readable" is different across languages), but the goal is the same.

Finding the privacy statement. The first, and most obvious, is that users need to be able to easily find the privacy statement. Having a privacy statement is required across the board in privacy regulations, therefore it is also in any organization's interest to have it prominently displayed.

Here again these laws do not generally prescribe exactly where this statement should be, but OTA has advocated for years that this link should at least appear on the homepage, a practice followed by 90% of organizations. While the remaining 10% of organizations in the U.S. were not *legally* required to have this at the time this study was conducted, it will be in their interest to display the privacy statement as prominently as possibly in the future based on these new regulations.

Layered privacy statements. Two other standards OTA advocates are also related to the general concept of readability. Statements should be "layered," which allows the user to find specific parts of the statement easily. This can be accomplished with something as simple as a table of contents, but ideally the use of links and other design techniques to make the privacy statement as readable as possible would help organizations ensure they are following these new standards around the world. In our Audit, less than half (47%) of the organizations had even a basic version of layering.

Use of icons. Another aspect of readability OTA advocates is the use of icons to indicate the types of information being conveyed by the text. Here again privacy laws rarely prescribe to this level of detail, but the concept is still important and just 2% of audited organizations used icons. Part of the reason for this is at the moment there is no global standard for icons, but OTA still recommends icons as it helps readers at different education levels, and even in different languages, understand and navigate the privacy statement more efficiently.



Multi-lingual support. On a related note, OTA also looked at whether the privacy statements were available in different languages – only 3.5% of organizations offered this. One explanation for such a low adoption rate is that some organizations may be using browser settings or location information and changing the language accordingly. Regardless, it will become increasingly important that statements be available in multiple languages as privacy regulations evolve around the world.

Ease of understanding. Finally, for the first time in 2019 OTA tracked the concept of "readability" directly. OTA analysts scored each statement and 32% of organizations had "readable" statements based on OTA standards. Privacy regulations around the world all have readability requirements, though they differ in how they define this. Regardless, organizations must understand these standards and ensure that their statements fit them, which most do not according to OTA.

Keeping Statements Up to Date and Notifying Users of Changes

Another important aspect included in all of these privacy regulations is that users are informed of changes to the privacy statement. Each regulation has different requirements for this, and two OTA recommendations relate directly to this concept.

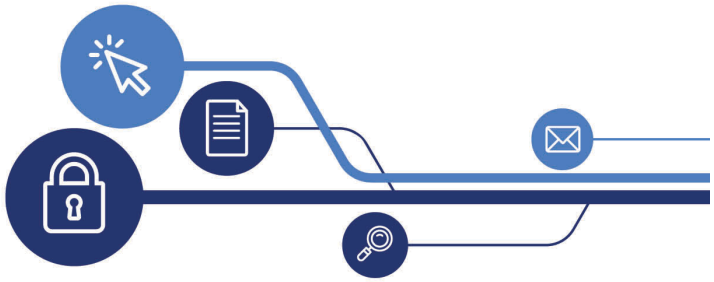
Date stamps. OTA has long advocated it is important to have a date stamp somewhere on the privacy statement (ideally at the top) to show users the effective date of the statement. Overall, 70% of organizations had a date stamp somewhere on their page – 46% had the stamp at the top, 22% had the stamp at the bottom, and 2% had it on both top and bottom.

In a report earlier this year,[6] OTA analysts also looked at how "fresh" these organizations' date stamps were. Fully 70% of statements had a date stamp on or after 1 January 2018. OTA does not advocate date stamps should be up-to-date simply for the sake of appearance, but as privacy rules continue to change around the world organizations need to be far more aggressive in making sure their statements are up to current standards.

Access to prior versions. The final OTA recommendation – offering users archives of previous privacy statements – covers the concept of allowing users to see what has changed. Unfortunately, only 3% of organizations in the Audit had some version of an archive or ability to compare the current privacy statement to prior versions.

This is particularly important as privacy rules around the world evolve. Privacy statements will need to be revised and it is in the interest of organizations to make it easy for users to see the changes. It could also relieve some of the burden on organizations to constantly inform users of changes to the privacy statement, something they are required to do under the three regulations discussed here. A simple archive would likely fulfill most of the requirements.

6 https://www.internetsociety.org/blog/2019/08/how-fresh-is-that-privacy-statement/



Conclusion

Privacy regulations around the world are evolving. Just within the United States, at least 11 states have privacy laws in motion, including California's which goes into effect in January 2020 and is covered in this study. Countries with new or emerging privacy laws include (but are not limited to) Brazil, China, Portugal, and Thailand. It is in every organization's interest to keep abreast of these laws as they change.

Privacy statements are only one piece of an organization's overall privacy practices, but the content of the statements themselves could bring penalties if they are not following the standards of these privacy laws.

How would your organization do in the Online Trust Audit? Check out the Best Practice Checklist (Appendix E)[7] and use it to improve your site's security and privacy.

About the Internet Society's Online Trust Alliance (OTA)

The Internet Society's Online Trust Alliance (OTA) identifies and promotes security and privacy best practices that build consumer confidence in the Internet. Leading public and private organizations, vendors, researchers, and policymakers contribute to and follow OTA's guidance to help make online transactions safer and better protect users' data. The Internet Society is a global nonprofit dedicated to ensuring an open, globally connected, trustworthy, and secure Internet for everyone.

7 https://www.internetsociety.org/resources/ota/2019/2018-online-trust-audit-and-honor-roll/