DOI:10.1145/3727636

Sebastian Zimmeck

Privacy

Beyond the Checkbox: Upgrading the Right to Opt Out

Creating a digital ecosystem that respects people's individual autonomy.

INCREASINGLY, PRIVACY LAWS give people privacy rights. Among those is the right to opt out.[a] The right acts as a gatekeeper for what data enters the ad ecosystem and what data stays outside. While some people make use of their right, for example, per the California Consumer Privacy Act, most do not. Even for those who do, the process is often difficult, time-consuming, and non-transparent. It should not be that way. How can we make the right to opt out work for everyone? How can we upgrade the right to opt out?

Making People Aware of Their Rights and Making Data Collection More Transparent

One major obstacle, which I think privacy researchers often neglect, is that many people are simply unaware of their rights and who is receiving their data. We cannot expect people to understand the obscurities of the online ad ecosystem, which is generally not transparent and based on an information asymmetry that is leaving people in the dark. Making people aware of their rights and bringing data collection practices to the surface would go a long way. Which begs the question: Where are the privacy influencers? We have lots of online personalities evidently dedicating their lives to dog sweaters. Yet, data privacy is not of interest? Given that it is unlikely that "Unboxing My Ad Profile!" will go viral anytime soon, we can focus elsewhere. For example, a substantial step in the right direction is the California opt-out icon,[3] as shown in the accompanying figure. Icons such as these should be displayed more prominently and not hidden in the footer of a website. App stores should prominently integrate them on app download pages and inside apps. In short, wherever people have rights, we should notify them of those in an obvious and easy-to-understand way.

Improving the Usability of Mechanisms to Exercise Rights

Icons, labels, and other notices must be actionable. As it stands, the right to opt out is too complicated and too time consuming to exercise. People are not able to exercise their rights at

a I am using the term "opt out" throughout this column as a shorthand for people's preference to have their data not shared or sold or used across different contexts for targeted advertising, including the right to object per the General Data Protection Regulation, Article 21, and similar rights that are technically "opt in" or "neutral" rights.

Example opt-out icon.

scale given the number of organizations processing their data.[5] So, how can we empower people? Usability is key. We should not blame people when systems fail.[4] Privacy, just as security, is a secondary task. People do not go on the Internet to "do some privacy." Thus, to make the opt-out right work it must be usable. This means that we have to write laws with an eye toward the technologies implementing them. We cannot just write laws without considering the systems they intend to govern and expect they will magically result in a privacy paradise. Rather, privacy laws must enable and necessitate usable privacy rights implementations. The reverse is also true. We must develop our systems such that they inherently follow privacy laws, that is, they are private by design.[2] So, our job as privacy researchers is to implement privacy laws.

People must become active to exercise their rights. There is no way around it. They will need to do some privacy labor.[1] But we should keep it as minimal as possible. Generally, we have three design choices: opt out (people must change privacy-unfriendly defaults); opt in (people will get nagged to allow tracking); and neutral (there is no default one way or the other and people are forced to make a choice). Whatever option we choose, if we want people to make an intentional choice with legal validity, we generally need to disrupt them in their primary task. Also, there is another challenge. We are faced with an asymmetry of automation. Website and app operators can implement automated choice interfaces to record people's choices (for example, cookie banners, settings interfaces) while people cannot generally counter with an automated choice selection on their end. This creates a usability problem. What can we do? We need to automate choices for the people! People must be able to say "No" automatically and at scale. In the opt-out context this can be done, for example, by sending Global Privacy Control (GPC) signals via browsers and other user agents.[9]

Making people aware of their rights and bringing data collection practices to the surface would go a long way.

Privacy Is a Systems Property: Avoiding Wrong Layers of Abstraction and Other System Fixes

Further, rights, as currently encoded in privacy laws, put too much onus on individuals when many privacy problems are systematic.[5] Indeed, privacy is a systems property. If we want to make progress toward a more privacy-friendly Web as well as mobile and smart TV platforms, we need to take a systems perspective. For example, instead of requiring people to opt out from individual websites, there should be opt-out settings in browsers and operating systems. If a law requires individual opt-outs, those can be generalized by applying one opt-out toward all future sites visited or apps used, if a user so desires.[8]

Another problem is that the ad ecosystem is structured such that if people opt out, in many cases, their data is still being shared just as if they would not have opted out. The only difference is that in the latter case the data is accompanied by a privacy flag propagating the opt-out to the data recipient.[7] However, if people opt out, their data should not be shared in the first place! The current system relying on the propagation of opt-out signals and deletion of incoming data by the recipient is complicated, error-prone, violates the principle of data minimization, and is an obstacle for effective privacy enforcement.

Changing the ad ecosystem is particularly important as it is not only used on the Web but also on many other platforms. Companies and the online ad industry as a whole need to do better.

Aligning Privacy Laws and Technologies

Privacy-friendly systems require the alignment of law and implementation. While the Internet is global, it is subject to a variety of local privacy laws. This leads to fragmentation. Generally, privacy laws should have the broadest territorial scope. The E.U. applied this lesson by replacing the Data Protection *Directive* (which required implementation into national laws) with the General Data Protection *Regulation* (which is directly applicable in all E.U. countries). For the same reason, the U.S. should have a (strong) privacy law at the federal level. However, if that is not in the cards, fragmentation can also be reduced by enacting identical or substantially similar state laws. Thus, state legislators should aim for consistency. With enough states there will be positive spillover effects as the overhead for website and app operators of following a state-by-state approach is not worth the implementation effort. Whether a law has federal or state scope, it surely needs to bring real privacy improvements.

Given that laws in different countries and states do not all neatly align, privacy mechanisms ought to be adaptable to different jurisdictions. Such adaption is possible by assigning jurisdiction-specific meaning to mechanisms that are neutral or flexible in their meaning. For example, GPC signals can have different meanings depending on from where they are being sent. By turning on GPC, people can generally express their preference to have their data not shared or sold or used across different contexts for targeted advertising. However, legislators and regulators can assign GPC more specific meaning as they see fit per the requirements of the privacy laws in their jurisdiction. An alternative would be to design a more nuanced mechanism with dedicated settings for different jurisdictions, but such settings could be abused for privacy-invasive browser and device fingerprinting.

Given that laws in different countries and states do not all neatly align, privacy mechanisms ought to be adaptable to different jurisdictions.

Enforcing Compliance

The right to opt out will not be effective without effective enforcement. Thus, we have to create laws and technologies with enforcement in mind. The current mechanisms require excessive enforcement effort to detect violations. Usually, regulators rely on individual high-profile enforcement actions to send a message to the wider industry that rights violations will not be tolerated. This lack of comprehensive enforcement is due to another asymmetry: Violations are difficult to detect and require a lot of work while most violators have only little risk to be detected. Thus, ultimately, we should design our systems to be inherently enforceable and behave in a privacy-friendly manner.

Why Burden People with an Opt-Out Right?

One more point: Why are we burdening people with a right to opt out at all? Why not have mandatory laws that prescribe what websites and apps can and cannot do? Why leave the question for each individual to decide for themselves? The way I see it, the reason is that privacy protects people's autonomy. Some people may indeed prefer personalized ads[6] which, despite some progress in privacy-preserving ad serving, may require some amount of data disclosure. Others may genuinely prefer to pay for services or content with their data. There is certainly a minimum level of privacy protection that everyone should have no matter what. But it is also true that different people have different preferences. Striking the right balance between enabling people to make their choices while providing a high default level of privacy is key. Of course, minimizing reliance on data sharing by improving privacy-friendly ad technologies is desirable in any case.

We Need to Do More

We have not done nearly enough to meaningfully implement opt-out rights on the Internet. It is neither enough to have rights codified in the books nor to develop opt-out technologies that do not realize these rights. To be sure, we need strong privacy laws and should continue the privacy law-making effort of the last decade. But we also need to have privacy technology seamlessly integrated with the privacy laws. Both need to go hand-in-hand to be effective. Building a structurally privacy-friendly Internet is not just nice to have; it is a necessity. The Internet is a technology for the people and must respect their privacy rights. By aligning legal frameworks, automated opt-out mechanisms, and user-centric design, we can improve privacy on the Internet so that it respects peoples' individual autonomy. We have made some progress, but we still have a long way to go. The tasks ahead of us will be challenging, requiring work across disciplines and a true commitment for improving privacy. But the rewards—a more just and equitable digital future—are well worth the effort. C

References

1. Berjon, R. and Yasskin, J. *Privacy Principles*. W3C Group Note. (Mar. 2025); https://bit.ly/3S71Ak0
2. Cavoukian, A. *Privacy by Design: The 7 Foundational Principles*. (2009); https://bit.ly/4jmZWqp
3. Habib, H. et al. How to (in)effectively convey privacy choices with icons and link texts. In *Proceedings of the 2021 CHI Conf. on Human Factors in Computing Systems* (2021); https://bit.ly/3GOVySY
4. Norman, D. *Proper Understanding of "The Human Factor"* (Dec. 2023); https://bit.ly/42Yvjln
5. Solove, D. The limitations of privacy rights. *Notre Dame Law Rev. 98*, 3 (2023); https://bit.ly/3H1HtRX
6. Ur, B. et al. Smart, useful, scary, creepy: Perceptions of online behavioral advertising. In *Proceedings of the Symp. on Usable Security and Privacy* (2012); https://bit.ly/4kiRtVY
7. Zimmeck, S. Opting out may not prevent websites from collecting your data. *Medium* (July 17, 2021); https://bit.ly/3YepIVB
8. Zimmeck, S. et al. Generalizable active privacy choice: Designing a graphical user interface for global privacy control. In *Proceedings of the 24th Privacy Enhancing Technologies Symp.* (2024); https://bit.ly/3Fyxtzi
9. Zimmeck, S. et al. Usability and enforceability of global privacy control. In *Proceedings of the 23rd Privacy Enhancing Technologies Symp.* (2023); https://bit.ly/4dhZV5e

Sebastian Zimmeck (szimmeck@wesleyan.edu) is an assistant professor at Wesleyan University, Middletown, CT, USA.