Everything we thought we knew about privacy is wrong

Straight talk from a technologist and a lawyer about why, how and what next

Kasey Chappelle
Global Privacy Counsel
Vodafone Group

Dan Appelquist
Web & Internet Evangelist
Vodafone Group R&D

We were wrong, and we admit it. When we decided to make consent the primary justification for collecting and using personal information online. When we made privacy notices a legal document. When we defined "personal information" like so many angels dancing on the head of a pin. When we held companies accountable for their privacy policies, not their privacy practices. We created a monster . . . dozens of pages, thousands of words, hundreds of mobile screens of impenetrable legalese. Not something you expect to hear from lawyers or regulators very often, but there you go – we were wrong.

That's a sea change from what we've said over the past 20 years or so. ***Because things have changed.*** We've had enough experience to see the error of our ways. Frankly, it was hard not to, magnified as it was by technological developments that far outstripped policy improvements. We know now that ***we cannot expect users to read, understand and make meaningful choices about online privacy based on privacy notices alone.*** We're looking for a better way – information in context, automated controls, consistent user experiences across sites and services, and iconography that shows the way, even for our least sophisticated users. ***We cannot continue to secure privacy protections online only for our most tech-savvy and proactive of users.***

Meanwhile, online companies (web publishers, advertisers and other platforms) have become more technically proficient at tracking users in ways that most would agree can be damaging to online privacy, and that can occur even against explicit user intent. They do so using web technologies that were never designed to support user tracking but can be used (and abused) for exactly this purpose. And even old technologies see use so pervasive and so complex that a privacy notice cannot be the medium that we create real user choice and control. ***The technology landscape has changed too, and in ways that have placed users at a significant disadvantage.***

What in particular have we gotten wrong?

1. We've overly relied on consent and put all our eggs in the privacy notice basket.
2. We haven't made it easy – we've either hidden user choices behind multiple links and complicated requirements, or we've failed to give any meaningful choices at all.
3. Web user agents could have helped, but they have largely provided a bewildering set of choices and fragmented UI around technologies related to privacy.

Regulators observe what industry has done over the years with online privacy. They're reading reports like this one in the Wall Street Journal. And they see what the legal framework and its incentives have created. They're asking us to do better. In fact, they're insisting that we do better. Or they're going to step in with severe and comprehensive limitations on how we use online data – far more restrictive than what we might agree to today. Privacy by design is an overly ubiquitous buzzword today, [1] but its principles have real value in the web environment. If we can build privacy into the fundamental fibre of the internet, we can demonstrate a better, more user-friendly, more intuitive way to deal with personal data online.

[1] But it's a buzzword that our regulators have invested in. For example, see the resolution adopted last month by international privacy and data protection commissioners.

What should we be doing instead?

I. **Get back to basics.** Consent is only one reason why information might be collected and used online. And it's not a very good one. Information that must be collected, used and shared because the service won't work without it – what we're calling here primary purposes? A recitation thereof doesn't belong in the privacy notice.

One exception to this rule: If it wouldn't be obvious to the user that this information is necessary (for example, it's not collected directly from the user but from other sources). Or it's used in a way that some users might be inclined to complain about (for example, debt collection or fraud prevention).

A privacy notice should include only those pieces of information that:

a. Provide context (for example, where does this policy apply?)
b. Are legally required (identity of the responsible party, contact information)
c. Are nonobvious and necessary
d. Are secondary to the primary service a user has requested.

II. **Simplify and use icons.** For those collections and uses of data where consent is required, make descriptions as simple and consistent as possible. What that means, in essence, is that we can create the "Son of P3P" – once we've done the work of creating the privacy vocabulary (what needs to be disclosed and how), we've identified what's essential, and we can build the real interfaces that will convey that information in a meaningful and consistent format. Here's where policy languages and technical standards can play a role – but they can't stand alone![2]

III. **Give meaningful choices.** For those things that really require consent, the privacy notice doesn't end our obligations. Users should be able to grant that consent ***and*** they should be able to revoke that consent. That means choosing later on that they might not want to participate in our secondary programmes, without losing the services they take from us (within reason). Meaningful choice is almost never take it or leave it.

And this is where user agents can help. The user agent should be guiding users to make informed choices about their privacy in a consistent way. Modern user agents are already making great strides by furnishing users with asynchronous prompts, but the user experience of privacy is still fragmented and filled with code words.[3] User agents need to provide clearer information to users about how they are being tracked by persistent client-side data, and provide user control. W3C and other bodies may be able to play a role in providing a forum for

[2] We should build here on the in-depth work done by people like Lorrie Faith Cranor and her CUPS colleagues, by John Morris and Alissa Cooper of CDT, and by Aza Raskin and others at Mozilla.

[3] Users may understand that cookies have something to do with their privacy (if that's about all they understand about cookies), but as the Evercookie has shown, clearing cookies or using cookie browser settings does not ensure that they can't be tracked.

browser makers to compare notes and normalize language, but this should be an area of differentiation rather than standardization.

Can there be greater integration between privacy policies and user agents?

Here are some of the issues and next steps we'd like to explore through W3C. An increasing amount of information provided by the user agent on behalf of the user (such as location, camera image, calendar data) will be shared through the web with attached privacy meta-data and according to acceptance of privacy policies. In this world, does it make sense for the browsers to play an enhanced role in mediating user privacy?

Should web users be able to track, through their browser UI, the privacy policies they've agreed to and selectively revoke permissions given (in the same way that they can revoke permission to locate through the Geolocation API, for example)?

If not, then whose role is it to act on the users' behalf to inform and educate them about privacy threats and protect or warn them when their privacy is being curtailed?

So what are we proposing?

It's time to reopen the conversation. Technologists are understandably wary of reengaging on the issue of privacy, entwined as it is with the grey areas of law and policy. But lawyers and policymakers are realising that we can't do it alone. Without the technology and the standards that create the right privacy environment online, we won't achieve the goals we're all trying to hard to meet. So its time to examine and improve what's worked in the past, discard what hasn't, and discover what can be done moving forward. It's time for W3C and other standards bodies to look into what they can do to help. So we encourage W3C to create a privacy-specific Interest Group, one that can consider these issues across the board rather than the piecemeal treatment they've received up to now, and to take a strong stance in safeguarding user privacy on the web.

Appendix A

What does belong in a privacy notice?

Take out the fluff. Users don't need a recitation of all the data elements you've just collected from them on the registration page. They don't need to know that you'll use their email to respond to their customer support inquiry. And they don't care what your exact security protocols are or that you've disclaimed liability for any third party websites you've linked to.

1. Scope
   - Where can users expect this policy to apply?
2. Responsible entity
   - Who is the primary entity responsible for the data?
3. Non-obvious primary collection and use
   - Information collected directly from users and used only for the reasons the user provided it need not be disclosed in a privacy notice. Some examples:
     a. Service delivery
     b. Customer support
   - Disclose here information that it might have been necessary to collect from a third party (if not obvious in context) or ways that information might be used to support primary purposes that might not be expected or users might in some cases find objectionable. Some grey areas:
     a. Fraud prevention
     b. Debt collection
     c. Proactive law enforcement cooperation
4. Secondary collection and use
   - Information collected from or about users that might be used for other purposes. Some examples:
     a. Analytics and aggregated statistics
     b. Service improvement
     c. Collaborative filtering
     d. Personalisation
     e. Direct marketing
     f. Targeted advertising – first party
     g. Targeted advertising – third party
5. Choices users might have about secondary collection and use
6. Contact info
   - What must the user do to exercise their rights of access, correction and deletion?
   - Include at a minimum an email address.