

Friction for Privacy

Why privacy by design needs user experience design

Bart Jacobs, Hanna Schraffenberger,
Privacy by Design Foundation and iHub, Radboud University

6 dec. 2019

IRMA is an open source identity platform that is run by the not-for-profit Privacy by Design foundation in The Netherlands. It grew out of academic research at Radboud University Nijmegen – and originally at IBM Research at Zurich in the 1990s. IRMA is now clearly gaining momentum and is being integrated in various ways, especially in healthcare, (local) government, and also in commercial areas such as insurance. The techniques underlying IRMA have been developed with privacy protection as explicit goal. This article explores the impact of this privacy focus on the user experience (UX) and on the ongoing (re)design of the interface of the IRMA app. The authors are both closely involved in the development of IRMA.

What is IRMA?

IRMA is like a Swiss army knife for identity. It offers attribute-based authentication and signing, while encryption with IRMA is in a prototype phase. Here we concentrate on authentication, that is on proving who you are, especially in an online environment.

When first installed, the IRMA app is an empty wallet. The user can subsequently fill it with personal attributes, such as name, date of birth, address, email, mobile phone number, etc. These attributes come from multiple trusted sources and are stored in the user's IRMA app with a digital signature (of the source), so that integrity and authenticity of attributes are guaranteed.

The privacy-preserving character of IRMA depends on two main features in its technical design.

- A user can *selectively* disclose attributes. For instance, in order to watch a certain movie or play a game online, the user discloses only the attribute that he/she is older than 16, or older than 18, and nothing else. This is fully in line with the GDPR's data minimization requirements. We call it *contextual authentication*: a website asks the user to reveal certain attributes, appropriate and necessary for the relevant service, and the user can agree in his/her own IRMA app to the request and disclose these attributes (or not).
- Attributes of an IRMA user are stored *exclusively* in the IRMA app on the user's phone, and nowhere else. When a user discloses (or receives) attributes, data are exchanged directly between the app and the service provider (as verifier, or as issuer, of attributes). There are no intermediate third-parties acting as privacy hotspot, like with Facebook Login or with iDIN (the joint authentication service of banks in The Netherlands). This means that the Privacy by Design foundation that is running IRMA cannot – and does not

want to – register where people are getting or showing their attributes or what their values are.

This strong (technical) focus on privacy is all very nice, but is it also the "killing" feature for the wide-scale adoption of IRMA? In our experience, it is not. Instead, the combination of the following five aspects contributes most to adoption: (1) functionality: does it allow users to do what needs to be done; (2) trusted data: can the app be filled with valuable attributes; (3) privacy protection: does it protect against excessive data disclosure; (4) low costs: users should not have to pay at all, and other stakeholders should pay minimally; (5) user experience: is the app pleasant, efficient and intuitive to work with. The development of IRMA has originally focused on the first points. Now that IRMA is no longer an academic research project and is being used in several live projects, our focus has shifted: providing a great user experience without sacrificing privacy has become one of our top priorities. In this article, we explore the interaction between UX design and privacy-protection.

Designing for privacy

A first observation to keep in mind is that an authentication app like IRMA is only a *means*, not a goal in itself. It allows users to log in and to do the things that they are really interested in, namely buying or selling something online, watching a movie, etc. Developers and designers need to be modest in what they can demand from users, since the attention and patience that users will have for authentication are limited.

Our second, key point is that there is a dilemma when designing for privacy in authentication: In order to be widely adopted, the app needs to provide people with a smooth user experience and offer users an easy, efficient, intuitive way to disclose their attributes in order to get access. However, to support people in protecting their privacy, the user experience cannot be too smooth and intuitive, since that could make it too easy for people to use the app without really thinking about which information they are releasing and to whom.

Such a tension between user experience on the one hand and privacy on the other hand is not unique to IRMA. Since the introduction of the GDPR, it is hardly possible to visit any website without facing a cookie consent statement, which likely annoys the user and slows them down, but also provides them with at least some form of control over their browsing data.

One might think that we can learn from such consent examples. However, they rather illustrate precisely what we want to stay clear of: the use of design nudges to trick users into doing something which is mostly in the interest of the *website* rather than in their own interest, namely accepting rather than rejecting (tracking) cookies. This widely-spread design mechanism in user interfaces is called a "dark pattern". It steers people into directions that they typically don't wish to go. Dark patterns come in many forms. A popular example is visually highlighting the choice to agree with something (e.g., to share data for additional "services") while graying out the option to disagree. Also popular are pre-selecting "agree" as a default, or placing "obstructions", e.g., allowing users to agree to something with just one click but forcing them to go through a complicated settings menu to disagree.

At first sight, IRMA uses similar design nudges, in particular to keep users in the right flow for authentication: when asked to disclose the necessary information, the option to reveal the requested attributes is highlighted in a striking color, whereas the option to deny the request receives no particular emphasis. However, unlike dark patterns, the intention in IRMA is not to trick people, in the interests of IRMA, but to help them achieve *their own* authentication goal.

Of course, this does not mean that people should blindly agree to IRMA disclosure requests from websites. The GDPR does not allow excessive requests, since it requires data minimization. In this regard, people are protected by the law. But purely technically speaking, requestors can ask for any attributes that they desire, such as a passport number for the usage of a movie service. Since Data Protection Authorities (DPA) are not continuously monitoring the proportionality of every possible attribute request of websites, users also have their own responsibility to recognize potentially inappropriate requests (and to notify the DPA in case of over-asking).

Technology can help users with this challenge, but UX design can play a big role, too. From a privacy-perspective, a proper design triggers users to think critically about each new disclosure, makes them consider whether the request is appropriate and whether all requested attributes are necessary for the relevant service.

Deliberate friction

Unfortunately, relatively little is known about how to design for slow and deliberate decision-making, unlike for fast and non-reflective flows. With IRMA, we are currently exploring different options. One approach would be to alert and slow down the user upon first disclosure of attributes to a new website, for instance with a pop-up text: “You have not visited this site before; are you sure that you wish to disclose these-and-these attributes? Is it clear and fair what the site will do with your personal data? Have you checked the website’s privacy policy?” Subsequently, this choice could be recorded in the app, so that later disclosures to this same website can be handled more quickly. Similarly, a color-code could indicate that a request involves an especially sensitive attribute, such as a citizen registration number (called BSN in The Netherlands). While such design choices will not guarantee that people will carefully consider every single choice, they might help them to stop and think when it counts the most. Another addition that we foresee is a button that allows users to complain directly to the DPA about excessive attribute requests. Ideally, such a button will not only allow users to report abuse easily, but also will foster reflection about the information requests they face. Also, more patronizing strategies are possible. For instance, the app could pause, with a countdown timer, and confront users with a forced time-out reserved for reflection before allowing any choice to proceed. What these ideas have in common, is that when effective, they will cause friction rather than a smooth flow. They will cost users time and mental effort – things that UX design usually tries to reduce.¹

¹ For a broader and more theoretical perspective on how to design for privacy-decisions, with many relevant references, we refer to Terpstra, A., Schouten, A. P., de Rooij, A., & Leenes, R. E. (2019). Improving privacy choice through design: How designing for reflection could support privacy self-management. *First Monday*, 24(7). Available at <https://firstmonday.org/ojs/index.php/fm/article/view/9358/8051>.

The design mechanisms that we are developing for IRMA are meant to protect people from agreeing too easily to excessive attribute requests. They are like speed bumps and traffic signs on dangerous roads: they slow people down and demand attention for safety. We see it as a duty of care: IRMA is based on value-driven design and its design for privacy requires some slow-downs. A duty of care is especially relevant in situations with a significant knowledge asymmetry – which is often the case with digital technology. As part of this careful approach, also additional regulatory and technical means are being considered within the IRMA project to further protect user's privacy: for instance, certificates could be made compulsory for verifiers when requesting especially sensitive attributes like passport photos and certain registration numbers.

The design of IRMA is a continuous effort. However, some things have become clear already: first, IRMA needs to encourage slow and careful decision-making. Second, IRMA also needs to provide a fast route through the process, in those cases where the same attributes are disclosed to the same party each and every day. Time for deliberation is precious, and users should not be forced to ponder over the same choice every time.

In the end, determining how to resolve tensions between opposing goals requires experience in practice and tests with users, in order to see what actually happens when people's authentication data is placed in their own hands. What we have observed in tests so far is that young users typically navigate through the app quickly, try out buttons and learn about the app by observing what their actions do, whereas older users generally take time to understand what is happening, to access and read accompanying information, and to make sure to only tap a button once they know what it does.

Concluding remarks

What others can take from our experience is threefold: first, in order to make sure privacy-enhancing technologies effectively enhance people's privacy, these technologies need to be adopted, which requires a smooth user experience. Second, UX design for privacy differs from general UX design. Designers usually strive for interfaces that are intuitive, efficient and a joy to use. When aiming for privacy, other goals are relevant too, which ultimately might cause the experience to be less efficient, pleasant and smooth. Third, privacy-preserving characteristics in a system's technical design often put people in control over their data. People, however, do not necessarily use this control to actually protect their privacy – possibly even the opposite. User experience design can affect how people handle such control, either by stimulating users to give up information without thinking (e.g. via dark patterns), or by supporting them to reflect, by informing them, and by helping users protect their privacy themselves. All three insights boil down to one conclusion: privacy by design must include careful UX design.