How software developers can fix part of GDPR's problem of click-through consents

Björn Lundgren^{1,2}

Received: 13 March 2020 / Accepted: 18 March 2020 / Published online: 13 May 2020
© Springer-Verlag London Ltd., part of Springer Nature 2020

When General Data Protection Regulation of the European Union (GDPR) arrived, most people probably noticed a practical flaw in the privacy protection regulation. GDPR required that most agents desiring to use your information receive your informed consent—a seemingly reasonable requirement. However, overnight, Internet turns into a pop-up spam festival, with websites requiring approval for your personalized privacy settings. Although the requirement enables individuals to make detailed decision about what information to share, the process is always time consuming, often annoying, and sometime cognitively taxing. Practices of so-called ‘click-through agreements’ arguably increase the risk that individuals agree to a consent agreement without actually reading it (see, e.g., Grady et al. 2017, p. 858)—revealing a practical flaw in the GDPR regulation, in which individuals’ privacy fail to be properly protected.

It is fair to say that legislators could have benefitted from taking offline norms of informational distribution as a guide for an appropriate standard of online norms. Indeed, some have promoted an idea of the right to privacy as a right to “to live in a world in which our expectations about the flow of personal information are, for the most part, met” (Nissenbaum 2010, p. 231).¹ If we think of websites as agents that you interact with, it would be extraordinarily rare that agents in an *offline* situation ask for the type of permissions that agents ask for in an *online* situation (e.g., ‘Can I share information about all your romantic dates with 300 of my business partners?’). Indeed, in the offline world, we would never accept these kind of requests, nor the constant nagging repetitions of these request; we would expect more from both friends, family, and colleagues, even from strangers and commercial interests.

So how can we fix this? One the hand, we can wait for legislative fixes. However, legislative fixes can only do so much (e.g., add a requirement of a standardized consent form and that refusal of consent becomes simpler, etc.). More importantly, EU regulation mainly benefit EU citizen.² On the other hand, while we wait for legislative fixes, software developers—in general—and developers of web browser—in particular—can and *should* work to resolve this problem. Web browser can be utilized to save the ideal of these consent-agreements, by providing functionality that allows users to give pre-set responses to these types of requests; effectively solving the problem of click-through agreements. In addition, all web browsers should include automated functionality to deal with privacy-consent-requests based on the user’s contextually modifiable privacy settings. Furthermore, in line with ideas within the GDPR, developers of web browsers—and Internet services in general—should adapt to standards of *privacy by default* and *privacy by design*. Firstly, the standard settings for privacy sharing in the case of automated consent-requests should follow principles of privacy by default (i.e., nothing should be shared beyond what is necessary to make the website function properly—and there should be reasonable limitations on what type of information that can be accepted as necessary for functionality). Secondly, it should be possible for any user to adapt these changes as she sees fit (e.g., on websites of type x , allow for sharing $y_1, \dots, y_n$, under conditions $z_1, \dots, z_n$). Thirdly, Internet services should be designed with privacy considerations as a *prima facie* priority, which—although it seems obvious—is far from today’s common practice.

✉ Björn Lundgren
bjorn.lundgren@iffs.se

¹ Institute for Futures Studies, Stockholm, Sweden

² Department of Philosophy, Stockholm University, Stockholm, Sweden

¹ However, it can be questioned whether Nissenbaum’s idea holds in this case, because “expectations” may be given a fairly descriptive reading. Indeed, even if she is highly critical of various online information norms, her theory may, if applied, imply that the online norms are expected and hence appropriate.

² Arguably, privacy requirements for a large online market can have effects for citizens of other nations (and not only if they connect through an EU-based IP address).

Primitive examples of these types of functionality already exists (e.g., many web browsers have the ability to send a *do not track*-request to websites and some sets of websites also offer privacy-choice services that are pre-set for consent in accordance with previous choices on other sites) and there are various add-ons to increase privacy (e.g., by blocking various analytics functions). Some web browsers also attempt to compete through increased privacy protection, ranging from Opera's included VPN services (see, e.g., Williams 2017) to the more complex Onion Routing (Goldschlag et al. 1999) through Tor; so one may reasonably presume that there would also be a (niche) market for the above proposed services. Alternatively, one may think that Onion Routing through the Tor Browser is an ideal solution for privacy. However, although Onion Routing can benefit individual's privacy through anonymity protections, such anonymity protections does not protect the individual when she uses services that require the user to login (Lundgren 2020). Furthermore, de-anonymization technologies are becoming more and more powerful, enabling supposedly anonymized users to be re-identified (Lundgren 2020; Ohm 2010).³ An illustrative example is that of Johansson et al. (2015, p. 10), who "have shown how de-anonymisation can be achieved by analysing *when* a user posts information" with 90% successful identifications using machine learning and a sample of 1000 users (Lundgren 2020, p. 204). So, we cannot purely depend on technologies that aim to achieve technical anonymity, which—in turn—explains why we need web browsers to help enforcing proper consents.

Curmudgeon Corner is a short opinionated column on trends in technology, arts, science and society, commenting on issues of concern to the research community and wider society. Whilst the drive for super-human intelligence promotes potential benefits to wider society, it also raises deep concerns of existential risk, thereby highlighting the need for an ongoing conversation between technology and society. At the core of Curmudgeon concern is the question: What is it to be human in the age of the AI machine? -Editor.

References

- Goldschlag D, Reed M, Syverson P (1999) Onion routing for anonymous and private internet connections. *Commun ACM* 42(2):39–41. <https://doi.org/10.1145/293411.293443>
- Grady C, Cummings SR, Rowbotham MC, McConnell MV, Ashley EA, Kang G (2017) Informed consent. *N Engl J Med* 376(9):856–867. <https://doi.org/10.1056/NEJMra1603773>
- Johansson F, Kaati L, Shrestha A (2015) Timeprints for identifying social media users with multiple aliases. *Secur Inform.* <https://doi.org/10.1186/s13388-015-0022-z>
- Lundgren B (2020) Beyond the concept of anonymity: what is really at stake? In: Macnish K, Galliot J (eds) *Big data and democracy*. Edinburgh University Press, Edinburgh, pp 201–216
- Nissenbaum HF (2010) *Privacy in context: technology, policy, and the integrity of social life*. Stanford Law Books, Stanford
- Ohm P (2010) Broken promises of privacy: responding to the surprising failure of anonymization. *UCLA Law Rev* 57:1701–1777. <https://ssrn.com/abstract=1450006>
- Williams M (2017) Opera VPN review. *Techradar* December 25. <https://www.techradar.com/reviews/opera-vpn>. Accessed 30 Apr 2020

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

³ Therefore, one often speaks of 'pseudo-anonymization' instead of 'anonymization' in such situations.