Centre for Information Policy Leadership
Hunton & Williams LLP

Byline

July 2, 2015

Empowering Individuals Beyond Consent

by Bojana Bellamy and Markus Heyder

Originally appeared on the IAPP's Privacy Perspectives


Individual consent to data processing has been an anchor of data protection and privacy laws around the world. The assumption is that consent ensures that information practices are focused on the rights and interests of individuals by enabling them to control the use of their personal data. Most lawmakers resort to the consent-based model by default.

But is consent really the best and only way in this modern Information Age to provide meaningful control and to protect the individual?

This question is arguably the most burning question in data protection today. It is particularly relevant at a time when the legislative process on the new European Data Protection Regulation is entering the final furlong and other countries are revising their privacy laws (Japan) or legislating for the first time (Brazil).

We do not believe that consent is the best or only way to empower individuals in this day and age for three reasons.

First, consent has become overused and an over-relied-upon in practice, calling into question its function as indicator of meaningful individual choice and control. Privacy policies and notices are too numerous, long and complex to result in valid consent. In their efforts to cover all possible scenarios, comply with multiple variations of national privacy laws and avoid legal liability for deceptive practices, organizations feel compelled to cram their privacy policies with information that can neither be absorbed by ordinary mortals nor empower them to make valid choices. While privacy policies will always have their place in protecting organizations from legal liability, they do not effectively protect individuals or provide them with real control.

The solution to this problem will not simply be in developing shorter and better privacy policies in order to obtain more valid consent.

Second, modern information practices are on a collision course with canonical consent requirements as envisaged in many data privacy laws today. Increasingly, there are situations where consent will simply not work because:

- The context makes it impossible to obtain valid individual consent, such as where there is no direct interaction with individuals or individuals may not have a relationship with organizations that may touch their data in the context of machine learning or in an ecosystem of mobile devices and the Internet of Things (IoT);

- The context makes consent inappropriate, such as in fraud prevention or information systems and network security, where seeking consent would prejudice the very purpose of processing;

This article presents the views of the authors and do not necessarily reflect those of Hunton & Williams LLP or its clients. The information presented is for general information and education purposes. No legal advice is intended to be conveyed; readers should consult with legal counsel with respect to any legal advice they require related to the subject matter of the article.

- The practical implementation of a consent requirement would unduly burden individuals, such as where consent requests by multiple organizations in some online service ecosystem would constantly interrupt and seek the attention of individuals as they go about their daily lives, especially in connection with processing that is expected.

As Airbnb's Douglas Atkin eloquently said, "In the distant future, we'll forget the idea of engaging in technology at all. We'll swallow it, absorb it and wear it, without us really thinking we're engaging in technology per se."

How would consent and individual control look in a world where we will not specifically engage in technology but the technology becomes part of us and everything around us?

Third, and perhaps most importantly, are other mechanisms in our ever-growing privacy toolkit and existing legal regimes that, in the appropriate contexts, are able to deliver privacy protection and meaningful control more effectively than consent. However, while these alternative mechanisms already exist, they must be better understood, further developed and more broadly accepted.

Policy-makers and lawmakers, as well as privacy regulators, should be shifting a significant portion of their attention from consent to these other mechanisms and safeguards. And organizations, in turn, must be prepared to embrace such alternative and innovative ways to deliver privacy and empowerment to individuals. Of course, there will always be situations where freely given and specific consent will be appropriate and the only way to use people's information. However, these situations are limited and must be narrowly construed to ensure the validity of the consent.

Here are some of these additional mechanisms and "individual empowerment" tools that we believe will play an increasing role in the Information Age. They will allow organizations to manage data in a way that truly focuses on the individual, provides more effective compliance and privacy protection and facilitates actual individual control in appropriate circumstances.

- **Legitimate Interest Processing**. European privacy laws already provide for a range of alternative legal bases for data processing that are on equal footing with consent. These bases include performance of a contract, legal obligation, vital interest of individuals, public interest or exercise of official authority and, crucially, legitimate interests of the controller or a third party, provided that individuals' rights and freedoms are not prejudiced. Legitimate interest-based processing is particularly relevant as it provides the necessary flexibility to face future technology and business process changes, while requiring organizations to be proactive, think hard and consider and mitigate risks and harmful impacts on individuals as they process personal data. Legitimate interest processing can legitimize many ordinary business uses of data, such as improving and marketing a company's own products or services, or ensuring information and network security. It also plays an increasingly significant role in the context of Big Data, the Internet of Things and machine learning by enabling beneficial uses of data where consent is not feasible and the benefits of the proposed uses outweigh any privacy risks or other harmful impacts on individuals. In its Opinion of April 2014, the Article 29 Working Party underscored legitimate interest-based processing as an example of true organizational accountability and responsible data management and provided specific guidance for organizations.

- **New Transparency**. Notice and consent have often been conflated. The time has come to firmly separate the two as stand-alone requirements. While there cannot be meaningful, informed consent without full notice, there can be useful and effective privacy policies where consent is neither sought nor necessary. Many legal regimes already treat notice as a separate legal obligation from consent. That distinction should be further emphasized and clarified to facilitate a transition from traditional privacy policies to new and effective transparency that clearly communicates an organization's information practices in the Information Age. Of course, traditional privacy policies and legal notices

© 2015 Hunton & Williams LLP

will continue to exist as matter of discharging an organization's legal obligations. However, new transparency will go beyond what's required in a legal notice, focusing on individuals and explaining the current and potential uses of data in a way that makes sense. It will address future uses that are not yet known and any associated concerns. It may explain the rationale and benefits of additional uses of data as a matter of customer relationship and be presented in an innovative and user-friendly manner, through dashboards, portals, interactive apps and, where required or possible, may set forth innovative ways to exercise choice and control.

- **Focus on Risk and Impact on Individuals**. Risk management and the need to understand, assess and address risks and harmful impact to individuals is fast becoming an integral part of organizational accountability and increasingly a legal obligation in many privacy laws. From formal data privacy impact assessments and privacy by design for new products and services, to consideration of risk and harm to individuals when deciding on appropriate security measures or on whether to provide breach notification, risk is an integral part of how organizations prioritize and implement their privacy compliance programs. This approach puts individuals firmly at the center of an organization's information management practices and results in better protection and compliance for individuals, especially in contexts where individual consent is neither required nor feasible.

- **Individuals' Rights to Access and Correction**. Access and correction rights are important elements of individual control and central to many data privacy regimes around the world. The ability of individuals to have access to their data and be able to correct inaccurate or obsolete data is an essential mechanism of control that should be made available as widely as possible. Access and correction are also intrinsically related to transparency and organizations may be able to innovate here too.

- **Fair Processing**. Fair processing is a stand-alone data protection principle in many data privacy laws in Europe and beyond. Over the years, practitioners and regulators have equated fairness with providing privacy notices to individuals. Fair processing, however, goes beyond privacy notices and we believe the time has come to resurrect this principle back into practice. In its 2014 report on big data and data protection, the UK Information Commissioner's Office (ICO) elaborates on the concept of fair processing in the context of big data. The ICO suggests organizations should consider factors such as whether the proposed use was known or reasonably "expected" by individuals, whether it may result in "drawing conclusions or making decisions about individuals," whether individuals were deceived or misled about how their data will be used, the impact of the proposed processing on the individual and the integrity and accuracy of data. These fair processing factors ensure that information practices are focused on the individual data subject and go a long way in effectively protecting the individual from harmful impacts.

We have over-relied on consent at the expense of other individual empowerment mechanisms and tools. We have overburdened individuals and deputized lay people to play privacy professional in contexts that are increasingly complex and difficult to follow. Plus, we have underestimated the need to adapt our privacy principles to the rapid changes that technology is bringing to society.

Deployed appropriately, alternative tools can enhance the value of consent by limiting its use to situations where indicating actual agreement is actually possible and meaningful. Where this is not the case, the hard work on privacy must come from these alternative tools and from responsible practices of accountable organizations, but without ever losing the focus on the individuals whose personal data are being used. The many ongoing processes to reform existing privacy regimes and to create new ones provide an opportunity to get individual empowerment right.

© 2015 Hunton & Williams LLP