Bloomberg BNA

Privacy and Security Law Report®

Data Transparency

Transparency has been a fundamental concept and requirement in many data privacy laws around the globe and is often expressed through the concept of ''notice'' to individuals. There will be an ever growing need for true transparency that gives individuals the necessary information to make appropriate choices about sharing their personal information and the confidence that their data are being used for legitimate purposes and with the appropriate protections, the authors write.

User-Centric Data Transparency for the Trusted Information Age

BY BOJANA BELLAMY AND MARKUS HEYDER

Transparency is front and center of most privacy policy debates in our modern digital society and data driven economy. This is so for a very good reason: with the increasingly complex data ecosystem that undergirds our social and economic lives, transparency is the basis of individuals' trust and empowerment on the one hand, and sustainable and innovative use of data on the other.

Bojana Bellamy is the president of the Centre for Information Policy Leadership.

Markus Heyder is vice president and senior policy counsel of the Centre for Information Policy Leadership.

This article is based on the Centre for Information Policy Leadership's and Telefonica's joint white paper, ''Reframing Data Transparency.''

Transparency, of course, has been a fundamental concept and requirement in many data privacy laws around the globe. It is often expressed through the concept of ''notice'' to individuals. It requires organisations handling personal data to be open with and inform individuals of their data uses and practices. In the U.S., the Federal Trade Commission takes action under a theory of deception or misrepresentation against companies whose privacy practices do not correspond to their stated privacy policies and notices. In Europe, the new General Data Protection Regulation (GDPR) has adjusted the role of transparency within data privacy and enhanced the transparency obligations of organisations.

However, in their wish to achieve strict legal compliance, organizations have been forced to meet transparency obligations through complex and legalistic privacy notices that do not deliver actionable information to individuals. In turn, this failure can lead to the erosion of trust in the digital society and data economy. Individuals do not know what is happening to their personal data, they do not understand the value in data processing and do not take advantage of opportunities to make choices about how their data is used, even in contexts where such choices would be possible. From the perspective of companies, therefore, this lack of transparency and the resulting lack of control and ''digital trust'' becomes a critical economic and business issue. The

 ISSN 1538-3423

erosion of digital trust threatens to undermine the effective digitalisation of society and impede economic growth.

Thus, many organisations are now developing new transparency approaches that go beyond traditional privacy notices and embed the information about their data practices and policies within the user experience itself. For example, many companies now use dashboards, portals, apps and contextual information to provide information to their customers, especially in contexts where individual choice and consent are not practicable or effective but individuals must be given the confidence that their information will be protected nonetheless. Such companies aim to reassure their customers that their data is being used responsibly and in ways that respect their fundamental rights and freedoms. These emerging approaches to a more user-centric transparency are better suited to create the necessary buy-in from individuals and society to legitimate and beneficial uses of personal data. They truly empower individuals, while at the same time providing increasingly better digital services.

However, successfully devising actionable, user-centric transparency requires a dynamic approach. Stakeholders must continuously assess, reassess, research and develop innovative transparency solutions that are capable of building public trust as well as satisfying context-specific transparency needs.

Organizations have been forced to meet transparency obligations through complex and legalistic privacy notices that don't deliver actionable information to individuals.

The mission to deliver effective and user-centric transparency as well as user controls is at the heart of many current initiatives. For instance, various projects of the Data Transparency Lab, as well as dashboards and apps from companies, such as Alphabet Inc.'s Google, Facebook Inc., Vodafone Group PLC and Movistar, enable customers to review, monitor, download or analyse how their data is used. The 2015 EU-US Privacy Bridges Project explored, among other topics, the issue of data transparency. Finally, organisations preparing for the implementation of the GDPR are starting to consider the enhanced transparency obligations under the new requirements.

Building on these initiatives, the Centre for Information Policy Leadership at Hunton & Williams LLP (CIPL), a global privacy and information policy think tank based in Brussels, London and Washington, DC. and Telefónica, one of the largest telecommunications companies in the world, recently issued a joint white paper on ''Reframing Data Transparency.'' The paper was informed by an earlier experts ''roundtable,'' with business leaders, data privacy officers, data privacy regulators, technologists and academics.

As reflected in the paper, there is broad consensus that a new user-centric delivery of transparency is indispensable to a well-functioning digital society. The following are important themes and points from the paper.

There is a Transparency Deficit in the Digital Age

In the age of connected homes, smart cities, ubiquitous mobile devices, artificial intelligence, machine learning and ingestables and wearables, it is difficult for organizations to meaningfully and effectively inform people of their data practices using traditional privacy policies and notices and related tick-box approaches. This results in a growing gap between traditional privacy notices and what individuals need: user-centric transparency that is capable of delivering understandable and actionable information concerning an organization's data use policies and practices, what the benefits of such use are to individuals and society, how the organization protects the data and how users can manage and control the use of their data. This gap results in a transparency deficit that undermines customer trust and their ability to participate more effectively in the digital economy.

User-Centric Transparency Requires Reframing of Traditional Approaches to Transparency

In a connected world, where there may be no direct relationship between companies and their end-users, both transparency and consent as a basis for processing are particularly challenging. Indeed, in the data-driven economy, there must be, by necessity, an increasing reliance on organizations to protect individuals without his or her input or consent. Thus, a new user-centric approach to transparency is necessary not only to enable effective consent by individuals where consent is still feasible and effective, but also to build the trust in cases where consent is not feasible or effective. In such cases, the role of user-centric transparency is to inform and reassure individuals that the organization will use their data responsibly and subject to specified accountability measures and, hence, to create trust.

It is crucial to consider the timing of transparency communications and measures.

This requires renewed focus on exactly what information should be shared with individuals, how it should be shared, and when it should be shared to accomplish this task. The relevant considerations include what information will most effectively tell individuals how and why their personal data is being processed, i.e., what are the really important facts and information that the individuals actually want to and should know?

The nature of transparency should be driven by the concerns of individuals and the particular data use context, rather than by traditional legal notice requirements. Individuals should also be informed about any unexpected uses of their data or uses that may compromise their fundamental rights and freedoms, as well as how the risks of such uses are going to be mitigated. It

  PVLR ISSN 1538-3423

is also important to recognize, however, that transparency cannot be absolute or impede other fundamental rights and legitimate interests. For example, commercial considerations, such as trade secrets and intellectual property rights, may impose limits on disclosing certain data handling practices.

Moreover, certain forms of transparency, such as disclosing the data or processing algorithm, may be counter-productive as such disclosures may not actually lead to a better understanding of the data handling and decision-making processes. The public's legitimate questions and lack of understanding about algorithm-driven processing operations should be addressed by other means.

For example, organisations can implement strong organizational accountability frameworks, which, among other things, will provide individuals with meaningful information and reassurances about the safeguards that the organization applies to algorithm-driven processing operations, including safeguards that are ''baked'' into the processing operations from the outset. They can also develop simple and seamless ways in which individuals can easily exercise their rights of access, correction and redress, where appropriate. Effective ways for organisations to provide user-centric transparency about their data practices include layered transparency notices and new forms of contextual and embedded transparency measures and tools.

It is also crucial to consider the timing of transparency communications and measures. Currently, many organisations provide individuals with information about their data practices at the time of first contact or transaction. However, most individuals cannot make an informed decision about whether or not to share their personal data with companies at that point in time. Also, customers may feel pressured into accepting the data practices of the company at that moment, given that many companies bundle their general terms and condition with their privacy notices. One solution would be to deliver transparency by using several transparency measures at various key times before and during data collection, and also during the lifecycle of data use. Transparency tools should be designed so that they are permanent tools which are available to individuals at all times.

Organizations must be proactive and take a leading role in innovating on how to deliver user-centric transparency.

User-Centric Transparency is a Multi-Disciplinary Endeavor

Transparency can no longer be viewed as a mere legal issue that can be addressed by satisfying traditional notice requirements. Instead, it is a considerable multi-disciplinary challenge requiring not only input from the traditional privacy stakeholders, such as regulators, organisations and individuals. Equally, creating and delivering user-centric transparency and tools will no longer be the prerogative of the company's legal departments. Increasingly, it will require the expertise and engagement of experts from other relevant disciplines, including behavioral economists, social scientists, psychologists and user experience specialists. Organisations will have to learn how to view transparency through business and customer relationship optics.

Naturally, because data transparency is a critical business issue, organizations must be proactive and take a leading role in innovating on how to deliver user-centric transparency. Data-driven companies must research and develop effective transparency approaches. They will have to become more fluent in explaining the value exchange and benefits of data processing to individuals. This, in turn, will boost trust in digital services, broaden user support for more expansive but beneficial uses of their information, and enable people to more fully support, participate in, and benefit from the digital age.

Data Protection Authorities Have a Key Role

DPAs have a key role in promoting and incentivizing effective data transparency approaches and tools. This requires that DPAs engage in ''smart'' data regulation. This means that DPAs should promote progressive and future-proof rules and laws that protect both fundamental rights and the ability to innovate. They should be selective and adopt a risk based approach to their supervision, advisory and enforcement powers. Finally, they should adopt a more collaborative approach to compliance and engagement with industry and proactively incentivise and showcase the best practices of delivering a user-centric transparency.

This also means that organisations should expect increased transparency towards the regulators, so that regulators can perform their oversight and enforcement obligations from a foundation of knowledge and trust.

Individuals must be empowered through broader digital literacy

It is crucial to support and enhance the general digital literacy of individuals. Such literacy would include an understanding of the uses of personal data and the societal and individual benefits of data processing. It will also promote awareness of relevant data privacy rights, such as right of access, correction, objection and how to exercise them, as well as the understanding of the data management tools available on the market.

Digital literacy education is not the primary responsibility of individual companies, although they have a significant role to play. Digital literacy education should take place through schools, universities, consumer education campaigns, government bodies, regulators and industry. Finally, media has an important role to play in demystifying data and digital economy and delivering approachable and more balanced consumer education.

Clearly, a lot of work lies ahead of all stakeholders to create and re-create the kind of user-centric and actionable transparency that is required to support the modern information economy as it grows and changes. As our data-driven economy becomes ever more complex, vast and ubiquitous, there will be fewer opportunities (and less desire) for individuals to make moment-by-moment choices about how, when and by whom their data are being processed. But there will be an ever

growing need for true transparency that gives individuals the necessary information to make appropriate choices where still feasible, but, more importantly, the confidence that their data are being used for legitimate purposes and with the appropriate protections in place, even where they do not make specific choices.

  PVLR ISSN 1538-3423