A Call for Evidence on EU Data Protection Proposals by the UK Ministry of Justice Draft Regulation COM(2012)11 and Draft Directive COM(2012)10

Submission by the Information Technology and Innovation Foundation (ITIF)

March 6, 2012

About Us

The Information Technology and Innovation Foundation (ITIF) is a Washington, D.C.-based think tank whose mission is to formulate and promote public policies to advance technological innovation and productivity internationally and in the United States. Recognizing the vital role of technology in ensuring prosperity, ITIF focuses on innovation, productivity, and digital economy issues.

ITIF is pleased to submit these comments in response to the Ministry of Justice's Call for Evidence seeking views on the potential impact of the European Commission's proposal for data protection, published on January 25, 2012. The proposal contains two parts: a draft Regulation which would replace the 1995 Data Protection Directive (and which was implemented as the Data Protection Act of 1998 (DPA) in the UK) and a draft Directive which would replace the Data Protection Framework Decision (DPFD) which was agreed to in 2008. The draft Regulation applies primarily to individuals, businesses and non-profit organizations whereas the draft Directive applies primarily to the law enforcement and judicial sectors. We will limit our comments to the draft Regulation.

Overview

The approaches taken in Europe to privacy are clearly different than in the United States. In Europe, privacy is seen as a right, and as a right, it trumps other personal and societal values. In contrast, in the United States, many people see privacy as one value among many, and as such, must be balanced against other competing interests. While citizens and policymakers on different sides of the Atlantic may disagree on these broad frameworks for privacy, both may still seek common objectives: namely, creating policies that protect the privacy of the individual while minimizing the burdens imposed on businesses and other organizations.

With this in mind, we offer the following recommendations:

- Avoid regulations that negatively impact the Internet economy
- Consider the impact of regulations on future innovations
- Create regulations that specify outcomes rather than methods
- Avoid regulations that impose excessive burdens on organizations
- Avoid broad industry-wide regulations when sector-specific regulations would be more appropriate

Avoid regulations that negatively impact the Internet economy

The proposed restrictions on profiling, such as those defined in Article 20, will negatively impact the Internet economy, particularly online advertising. Internet advertising supports the creation and maintenance of new online content, applications and services including news, videos, music, games, social networking, reference, email and other online services. Many of the most popular websites on the Internet would not exist today without online advertising. The top three most popular websites in the UK—Google, Facebook and YouTube—all use online advertising almost exclusively to support their products and services. The Internet ecosystem is a significant source of economic activity, and online advertising is the fuel powering this economic dynamo. ITIF estimates that the annual global economic benefits of the commercial Internet equal at least $1.5 trillion, more than the global sales of medicine, investment in renewable energy, and government investment in R&D, combined.[1] Policymakers should consider carefully any attempts to limit the use of online advertising, and its effect on the Internet at large, before tampering with the foundation of its growth.

The impact of regulations on the Internet economy is already evident. Academic researchers Goldfarb and Tucker analyzed the impact of the European Union's Privacy and Electronic Communications Directive (2002/58/EC) which was implemented in various European countries and limits the ability of advertisers to collect and use information about consumers for targeted advertising. The authors find that after the new privacy laws went into effect, the laws resulted in an average reduction in the effectiveness of the online ads by approximately 65 percent (where the effectiveness being measured is the frequency of changing consumers' stated purchase intent). The authors write, "the empirical findings of this paper suggest that even moderate privacy regulation does reduce the effectiveness of online advertising, that these costs are not borne equally by all websites, and that the costs should be weighed against the benefits to consumers."

---

1. Robert Atkinson et al., "The Internet Economy 25 Years After .com," (Washington, D.C.: Information Technology and Innovation Foundation, 2010), http:// www.itif.org/files/2010-25-years.pdf.

Targeted advertising is especially important for supporting the websites responsible for the majority of the free and low-cost content online. In particular, general-interest websites, such as news sites, have little ability to determine what ads their users would be most interested in without targeted advertising. (In contrast, some special-interest sites, such as sports or travel websites, can more easily provide contextual advertising.) Not surprisingly, Goldfarb and Tucker found that the negative impact on ad effectiveness from the European privacy regulations was strongest among these general interest sites. The negative impact was also stronger for non-obtrusive ads (e.g. smaller ads or ads not using multimedia). This finding suggests that small, text-based ads are significantly less effective unless they can be tailored to a user's interests. The authors also note that if advertisers reduced their spending on online advertising in line with the reduction in effectiveness resulting from stricter privacy regulations, revenue for online display advertising could fall by as much as half.[2] And as Beales notes, a reduction in ad revenue directly hurts online publishers since more than half of ad network revenue goes to publishers who host the ads.[3]

Restrictive data regulations would reduce revenue flowing into the Internet ecosystem, which means not only fewer websites and less valuable content, but also less spending by Internet companies on servers and bandwidth. The net result will be fewer jobs, less consumer welfare and lower productivity. In addition, if the Internet is less valuable to consumers because there is less useful content, applications and services, users are less likely to subscribe to broadband. This is not to suggest that all privacy regulations be avoided, but rather that policymakers should tread lightly and focus more on preventing harms from privacy violations than on legislating burdensome regulations.[4] The evidence clearly shows that more restrictive privacy regulations result in less free and low-cost content and more spam (i.e. unwanted ads) which is not in the interests of most consumers.

Consider the impact of regulations on future innovations

There is a fundamental problem with the current process for evaluating the draft Regulation since the Ministry of Justice is only evaluating how this will affect existing businesses and organizations. A more forward-looking process would assess not only the impact on existing businesses, but also on potentially new legitimate businesses and business practices that could be curtailed by these regulations. For example, the Ministry should evaluate how these

---

2. Avi Goldfarb and Catherine E. Tucker, "Privacy Regulation and Online Advertising," (2010) http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1600259.
3. Howard Beales, "The Value of Behavioral Targeting," 2009, http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf.
4. Daniel Castro, "Data Privacy Principles for Spurring Innovation," (Washington, D.C.: Information Technology and Innovation Foundation, 2010), http://www.itif.org/files/2010-privacy-and-innovation.pdf.

regulations might reduce data sharing, data analytics, and the creation of data-driven products and services. To take one example, Article 23 outlines a data minimization principle that discourages organizations from collecting data unless they have pre-defined plans for how they will use for this information. This requirement restricts organizations from conducting post-hoc analysis to develop new types of products and services based on what they learn from the data, even if these organizations use this data in a way that protects individual privacy.

To take another example, Article 20 outlines restrictions on profiling individuals, which may eliminate the possibility of developing and using certain personalized digital signage or types of electronic interactive displays.[5] Moreover, these restrictions on profiling are enhanced for certain special categories of personal data defined in Article 9. The draft Regulation defines these "special categories" to include data that relates to an individual's race or ethnic origin, political opinions, religion or beliefs, trade-union membership, genetic information, health, sex life, and criminal history. These restrictions on the collection and use of certain special categories of information means there is an entire class of targeted advertising that cannot be used. For example, these restrictions could potentially prevent or limit marketers from effectively creating targeted ad campaigns for services like online Christian bookstores, Brazilian music stores, or dating websites based on a particular faith or sexual orientation.

Stricter consent requirements might also impair the ability of organizations to develop new products and services. Currently many websites on the Internet operate use an opt-out model whereby consumers can review the privacy policy offered by an organization and then decide whether to use the services offered by that organization. The draft Regulation establishes explicit affirmative consent ("opt in") requirements for processing personal data, including for online services. Lundblad and Masiello have demonstrated that "opt-in is a rhetorical straw-man that cannot really be implemented by regulatory policies without creating a number of unintended side effects, many of which are suboptimal for individual privacy."[6] Specifically, the authors find that opt-in requirements encourage providers to broaden the scope of data they ask for, desensitize users to making decisions about sharing personal data, and raise the switching costs leading to less competition and lock-in. In addition, opt-in requirements create an administrative burden on organizations as they seek to offer new products and services as they must first ensure that every user has taken a proactive step before they can offer their customers something new. This means that organizations and businesses cannot rapidly develop and deploy new services, a hallmark of the Internet and information age. These types of regulations would effectively create speed bumps to innovation. Policymakers should

5. Digital signs use LCD, LED, and plasma screens to display advertisements in public locations such as shopping centers, hotels, and airports.

6. Nicklas Lundblad and Betsy Masiello, "Opt-in Dystopias," *SCRIPTed* 7, no. 155 (2010), http://www.law.ed.ac.uk/ahrc/script-ed/vol7-1/lundblad.asp.

endeavor to better understand the costs of opt-in before enacting this requirement and consider the merits of opt-out.

Create regulations that specify outcomes rather than methods

Where possible, regulations should remain flexible and require specific outcomes rather than specific business processes. Creating regulatory flexibility encourages companies to achieve compliance effectively and efficiently rather than just superficially achieving compliance the cheapest way possible. In some areas the draft Regulation achieves this goal. For example, the draft Regulation specifies clear guidelines to create transparent business processes and mandates performance-based data breach reporting and notification requirements. One example of how the draft Regulation fails in this manner is the requirement that some organizations employ a data protection officer. While designating an employee to this position may achieve some level of accountability and oversight, these types of risk-management decisions are best left to individual organizations. This requirement is also likely to be a burden to small companies. A better option would be to require functional outcomes, such as requiring a publicly-registered point of contact for data-related inquiries.

Avoid regulations that impose excessive burdens on organizations

The draft Regulation mandates that access to information stored about an individual be provided to individuals free of charge. Underlying this mandate appears to be an assumption that providing this information to individuals is feasible, low-cost, and privacy-enhancing. While many organizations have centralized and cross-linked information systems, such as integrated customer relation management (CRM) systems for customer data, for many organizations, especially smaller ones, this is not always the case. To put in place such systems would cost organizations considerable resources, not only to establish the initial systems but also to devote staff to managing information requests. Similarly, many organizations do not have processes or systems in place to verify the identity of individuals making this type of request. Although the draft Regulation does impose some limitations on the frequency of these types of data requests from individuals, the limitations are not sufficient to insulate organizations from potentially burdensome regulatory compliance costs. In addition, it is conceivable that citizen activists would use this requirement, or similar ones such as those to correct inaccurate information or to delete personal data, to subject organizations to harassment through frivolous requests.

Avoid broad industry-wide regulations when sector-specific regulations would be more appropriate

The draft Regulation also proposes a right to data portability. Article 18 declares a right to have personal data that is processed electronically to be provided upon request an electronic and structured format for reuse by the data subject. Data portability can be a useful tool to promote competition and innovations among information-based products and services. But it serves no apparent purpose for most information that websites collect on individuals. For example, do people really need their purchase history from Amazon.co.uk to be portable? Moreover, this requirement may be too cumbersome to implement and will be costly to implement. Information systems use and store data in varied and disparate formats and it may not be feasible to implement such a regulation across all possible sets of information systems. Instead, it would be better to implement industry-specific regulations that deal with the practical realities of different types of data. For example, health, financial and home utility data (e.g., electricity, gas and water) may be candidates for sector-specific data portability regulations.

Conclusion

The draft Regulation provides a detailed framework for data protection that contains many useful recommendations; however, it also falls short in a number of areas. We urge the Ministry to continue to seek out more data to better understand user behavior and tradeoffs as it relates to privacy and the use of personal data. The Ministry should also work to leverage existing self-regulatory efforts by the private sector to manage personal data and it should work cooperatively with these organizations. Working jointly, the public and private sectors can better protect individual privacy while also protecting the benefits to individuals and society that come from continued innovation.

For more information about these comments, please contact:

Daniel Castro, Senior Analyst

Information Technology and Innovation Foundation
1101 K Street NW, Suite 610
Washington, DC 20005
United States of America
Tel: +1 202 626 5742
Email: dcastro@itif.org