

For Privacy, European Commission Must Be Innovative

by Omer Tene

February 28, 2011

This post is part of "CDT Fellows Focus," a series that presents the views of notable experts on tech policy issues. This month, CDT Fellow [Omer Tene](#) [1] writes about the consultation launched by the European Commission to update the European Union Data Protection Directive. Posts featured in "CDT Fellows Focus" don't necessarily reflect the views of CDT; the goal of the series is to present diverse, well-informed views on significant tech policy issues.

In a way, the process undertaken by the European Commission to review the current framework applicable to privacy and data protection is akin to speeding on a highway at 100 mph while looking at the rearview mirror. The [consultation](#) [2] launched by the EC and comments filed by some of the main players (see, e.g., [here](#) [3] and [here](#) [4]) are strongly anchored in the text of the [EU Data Protection Directive](#) [5] ("EU DPD"), enacted in 1995, negotiated several years before then, and based on [documents](#) [6] dating back to the late 1970s. That was the era of [mainframe computers](#) [7] and [punched cards](#) [8]; long before PCs, the Internet, and mobile, not to mention cloud services, ubiquitous computing, smart grid, genetics and biometrics.

Building on acquired knowledge and proceeding with care in small increments is firmly rooted in legal culture. Ours is a discipline based on [precedent](#) [9] and cautious tweaking of existing texts. Torts, contracts, and even public law today are strikingly similar to those in Roman times or ancient Jewish law. Yet given the scope and pace of technological innovation over the past 40 years and its [massive impact](#) [10] on the collection, storage and use of personal information, it seems that an innovative mindset is needed to overcome some of the shortcomings of the current framework.

General structure

The EU DPD is a structure based on two pillars – fair information practice principles (FIPPs) and a regulatory bureaucracy – with an overarching concept of consent hovering above. The FIPPs are not unique to the EU DPD and are in fact almost ubiquitous. They come under different names and are clustered differently, but are essentially the principles of data minimization (collection limitation), purpose specification, use limitation, retention limitation, transparency, accuracy (data quality), individual participation (access, rectification and right to object), security and accountability. I don't think there's reason enough to delve into these, as they are largely agreed upon from Canada and the [US](#) [11], through Europe, Israel, South Korea, and Japan, come to Australia and New Zealand. To be sure, data minimization has come under stress in the era of ["big data;"](#) [12] and we have not fully figured out the principle of [accountability](#) [13] yet. But all in all, there is a great degree of convergence with respect to the FIPPs. Put another way: where the [US Department of Homeland Security](#) [14] is in accord with European Parliamentarians, who's to argue?

Much more discord surrounds the regulatory bureaucratic aspects of the privacy framework. Here, different jurisdictions vary significantly, with the EU leading the way with its "fully independent" supervisory authorities charged with enforcing the law *vis-à-vis* both private sector and state. The EU DPD is inundated with form filling and filing processes that currently occupy a vast ecosystem of regulators, data protection officers (DPOs), private sector lawyers, accounting firms, and consultants (to name a few). "Notifying" or registering data processing operations; approving cross border data transfers; executing "model clauses" or certifying "binding corporate rules" – are just some of the activities undertaken by privacy professionals. A bit like sorcery, this meticulous activity yields questionable benefits to anyone but the professionals engaged in it. As one CPO once told me: "I view the notification form filed annually with the data protection authority as an envelope for the filing fee; I'm happy to send them the check without the envelope." Little doubt remains, even among regulatory strongholds, that the EU DPD's bureaucratic processes must be greatly simplified.

This brings us to the challenging issue of consent. Consent is a wild card in privacy regulation:

difficult to tame but impossible to get rid of. It is a concept so intertwined with the meaning of privacy that one cannot exist without the other. Any privacy infringement presupposes lack of consent. You invade my privacy by lurking around my home and peeking through the window; yet if I invite you to my home you come as a visitor, a guest, not an infringer. If I use Google to search my date's name and seek personal information about her, I may be invading her privacy; if she volunteers medical information over a drink, I am a polite listener.

The EU DPD currently authorizes the processing (meaning collection, storage, use or transfer) of personal data based on "unambiguous consent" or "explicit consent" in the case of sensitive data. The problem, of course, is that consent is often illusory. The state does not need citizens' consent to process data about them; employers can obtain employee consent to anything save (perhaps) pay cuts; and businesses bury statements about privacy and data use in dense legal documents undecipherable to non-experts.

Some have called for the abolition of consent as legal basis for processing data in certain situations. That is, prohibiting certain data processing operations outright, with or without consent. I view this as highly problematic. Data processing can be justified based on "implicit" consent (e.g., Article 7(b) of the EU DPD: "processing is necessary for the performance of a contract to which the data subject is party") or with no consent at all (e.g., Article 7(c) of the EU DPD: "processing is necessary for compliance with a legal obligation" or Article 7(f): "processing is necessary for the purposes of the legitimate interests pursued by the controller"). But I do not think the converse is true: processing cannot be outlawed in the presence of consent. To be sure, consent must be real – that is, free and informed. If it's not free and informed, it's not consent; and many common situations fall into this category. But overruling individual choice where it is present is paternalistic and fails to capture the nonconsensual element of any privacy infringement.

In addition, current debate about consent is often fixated on opt-in vs. opt-out. I think the more salient issue is transparency. Consider what is a better expression of individual autonomy – signing a 36 page contract printed in font 6 which includes a hidden paragraph on data usage (opt-in consent); or receiving conspicuous, clear notice and being offered a simple, no cost right to refuse (opt-out)? The point is that opt-out is not inherently inferior to opt-in; it depends on the notice. The FTC recognized this in its recent [Report](#) [15] on Protecting Consumer Privacy in an Era of Rapid Change, noting: "Different mechanisms for obtaining opt-in and opt-out consent can vary in their effectiveness. Indeed, a clear, simple, and prominent opt-out mechanism may be more privacy protective than a confusing, opaque opt-in." I support searching for mechanisms to provide transparency and robust notice to individuals, such as [icons](#) [16], privacy [dashboards](#) [17], and [layered notices](#) [18] written in plain English. Improving consent, not doing away with it, is the right way to go.

Definitions

Every legal text is only as good as its basic building blocks – the definitions. Unfortunately, the definitions in the EU DPD are in danger of unraveling. Look no further than the most fundamental term – "personal data" – currently defined as "information relating to an identified or identifiable natural person (...); an identifiable person is one who can be identified, directly or indirectly (...)". Endless [debate](#) [19] has raged concerning the identifiability of an IP address or cookie and the use of anonymization to render data un-identifiable. Yet recent advances in analytics and [de-anonymization](#) [20] attacks have shown the [futility](#) [21] of the "personal, non-personal" dichotomy.

Moreover, it is the singling out of an individual for unique treatment (e.g., the pricing of a loan or targeting of an ad) based on his or her profile, even without the ability to unmask his or her name, which has significant privacy implications. It is precisely this "commodification" of individuals that Ruth Gavison warned about in her 1980 Yale Law Journal [article](#) [22], "Privacy and the Limits of Law." Arguably, a company purchasing individual "profiles" without even addressing such individuals by name inflicts a more severe dignitary harm than one associating profiles with identified individuals. After all, it is statements like "gather all the ones with the yellow badge" that led to the adoption of data protection framework in the first place. However, extending the EU DPD to apply to the processing of any form of data, personal or non-personal, seems like an over-expansion.

An additional dichotomy in need of review is that between [controllers and processors](#) [23]. Data protection law allocates responsibility and delineates duties according to a categorization of an organization as a "controller" or "processor." A controller, defined in the EU DPD as the party that "determines the purposes and means of the processing of personal data," is traditionally viewed as the owner of the database, the one who has a direct relationship with the individual and therefore locus of liability. The processor (or "mere processor") is traditionally perceived as a service provider, a servant to the master-controller, whose sole responsibility is keeping the data secure. Yet how far this description is from market reality today, where layer upon layer of service providers (processors?) undertake an increasing role in the clients' (controllers?) business processes, including providing consulting services, driving innovation, and managing change. Moreover, with the advent of cloud computing and its architecture as a stack of infrastructure, platform and software layers, the neat distinction between controllers and processors has muddled. This is a critical matter, since in the absence of a clearly identified controller the framework remains teetering without a focal point for responsibility/accountability.

An additional sticky point concerns choice of law. The EU DPD was initially adopted as a common market measure intended to harmonize data protection regulation and thus remove barriers to data flows among EU Member States. As practitioners in Europe know well, harmonization remains a utopian vision far from a reality where large multinationals struggle to reconcile sometimes conflicting regulations. In addition, application of the European framework seems overextended under Article 4(1)(c) of the EU DPD, which applies European law to a controller established outside of Europe processing the personal data of non-Europeans if such "controller (...) for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of [a] Member State." European regulators interpreted "use of equipment" broadly, applying the EU DPD for example where a US-based website places a cookie on the browser of a user in the EU.

The Article 29 Working Party, group of European regulators charged with enforcing the law, recently issued a [document](#) [24] analyzing choice of law under the EU DPD. Yet much confusion remains, and will continue to exist given the inherent geographic indeterminacy of data flows. Peter Hustinx, the European Data Protection Supervisor, recently [called for](#) [4] replacing the EU DPD with a [regulation](#) [25], European legislation with direct effect in Member States, to avoid the inevitable disharmony in transposition of a [directive](#) [26]. While an appealing prospect, such a regulation would be excruciatingly difficult to negotiate and agreed upon among 27 Member States.

Enforcement is a sore issue for the EU DPD. It is an open secret that the framework is largely [not enforced](#) [27]. Indeed, implementation of the EU DPD is probably highest among US based multinationals, which implement strict compliance programs for risk management purposes and as part of overall corporate governance schemes. To increase enforcement, mechanisms must be put in place to facilitate cooperation among data protection authorities; incentivize individual enforcement by consumers and consumer organizations; and engage the press.

Call in the engineers

These issues and others, such as the expansion of the EU DPD to the sphere of law enforcement and national security pursuant to abolition of the "pillar structure" under the [Lisbon Treaty](#) [28], pose very difficult problems for us lawyers to solve. Play as we will with the language of the EU DPD, "personal data" will remain an amorphous notion, consent a treacherous concept, and enforcement problematic. John Palfrey recently [called for](#) [29] new collaborative policymaking mechanisms in the context of use of social media by youth. I echo this call with respect to the EU data protection framework: to make real progress, let's call in the engineers.

[Next week, I moderate a panel on review of the EU DPD at the [IAPP Summit](#) [30] in Washington, DC, with Peter Hustinx, European Data Protection Supervisor; Thomas Zerdick, European Commission; Jacob Kohnstamm, Chairman of the Article 29 Data Protection Working Party and President, Dutch Data Protection Authority; and Artemi Rallo Lombarte, Director, Spanish Data Protection Authority and Vice-Chairman of the Article 29 Data Protection Working Party. Hope you can attend.]

-
- [European Union](#)
- [european commission](#)
- [Data Protection Directive](#)
- [CDT Fellows Focus](#)

Copyright © 2013 by Center for Democracy & Technology. CDT can be freely copied and used as long as you make no substantive changes and clearly give us credit. [Details](#).

Source URL: <https://www.cdt.org/blogs/privacy-european-commission-must-be-innovative>

Links:

- [1] <http://cdt.org/personnel/omer-tene>
- [2] http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf
- [3] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf
- [4] http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-01-14_Personal_Data_Protection_EN.pdf
- [5] <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>
- [6] http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html
- [7] <http://www.computersciencelab.com/ComputerHistory/HtmlHelp/Images2/IBM7094.jpg>
- [8] <http://www.cs.nott.ac.uk/~ef/ComputerXHistory/Peripherals/1967-PunchedCard-1330.jpg>
- [9] http://en.wikipedia.org/wiki/Common_law
- [10] <http://idpl.oxfordjournals.org/content/1/1/15.full>
- [11] http://www.ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf
- [12] http://en.wikipedia.org/wiki/Big_data
- [13] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf
- [14] http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf
- [15] <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>
- [16] http://www.nytimes.com/2010/01/27/business/media/27adco.html?_r=2
- [17] <http://googleblog.blogspot.com/2009/03/making-ads-more-interesting.html>
- [18] http://www.facebook.com/note.php?note_id=10150434660350301&id=69178204322
- [19] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf
- [20] http://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf
- [21] <http://uclalawreview.org/pdf/57-6-3.pdf>
- [22] <http://www.jstor.org/pss/795891>
- [23] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf
- [24] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_en.pdf
- [25] http://en.wikipedia.org/wiki/Regulation_%28European_Union%29
- [26] http://en.wikipedia.org/wiki/Directive_%28European_Union%29
- [27] http://www.fra.europa.eu/fraWebsite/attachments/Data-protection_en.pdf
- [28] http://en.wikipedia.org/wiki/Treaty_of_Lisbon
- [29] http://www.twcresearchprogram.com/pdf/TWC_Policy_Palfrey.pdf
- [30] https://www.privacyassociation.org/events_and_programs/global_privacy_summit/breakout_sessions_global_privacy_summit1/