Informal Note on Draft EU
General Data Protection Regulation
(December 2011)

This informal note comments on certain aspects of the widely leaked draft proposal to modernize the European Union's data protection legal framework, and in particular the draft General Data Protection Regulation (the "draft regulation"). It does not necessarily represent the views of the U.S. Federal Trade Commission ("FTC"), any FTC bureau or office, or any other U.S. government agency.

The entire draft proposal, which also includes a draft directive on police matters, appears to affect a broad range of transatlantic commercial, law enforcement, and other interests. This note does not address that full range of issues. It focuses instead on several aspects of the draft regulation relevant to the jurisdiction and activities of the FTC, which protects consumers, consumer privacy, and competition through enforcement, outreach, rulemaking, and policy initiatives. Nor does the note attempt to catalog the various positive aspects of the draft regulation. Instead, the note focuses on two overarching concerns: the draft regulation's potential adverse effect on the global interoperability of privacy frameworks, and the draft regulation's serious implications for regulatory enforcement activities involving third countries.

First, the note addresses two respects in which the draft regulation may adversely affect the global interoperability of national and regional privacy regimes. Part of this potential adverse effect could result from the degree to which the draft regulation promotes divergence rather than convergence on various substantive issues; examples include the treatment of data breach notification, children's privacy, and the proposed "right to be forgotten." Part could result from the draft regulation's treatment of cross-border data transfers.

Second, the note highlights several serious implications the draft regulation poses for regulatory enforcement. These include the draft regulation's potential to (i) interfere or block investigations by public agencies from third countries in a variety of areas, such as competition, consumer protection, and (ironically) privacy; (ii) hinder information sharing between U.S. and EU regulatory agencies; and (iii) undercut enforcement cooperation between European data protection authorities and privacy enforcement agencies in the rest of the world.

The European Commission's stated goal is to improve the legal framework for data protection in a technologically advanced, globalized world.[1] The draft regulation, however, contains provisions that may undermine that aim. Indeed, there may be greater value for consumers in Europe and around the world in a balanced, proportional approach to privacy and data protection

[1] Indeed, one EU official was reported recently in the press as saying, "With these proposals, the EU is becoming the de facto world regulator on data protection."

that encourages interoperability with other countries and regions, and recognizes the legitimacy of enforcement and other interests.

1. Interoperability

Recognizing the global nature of data flows and the challenges they pose for consumer privacy, the FTC, and the broader United States government, have actively worked to develop privacy mechanisms that increase global interoperability between different privacy regimes. To that end, the FTC has played an active role in several recent international initiatives, such as the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules and the Accountability Project led by the Center for Information Policy and Leadership. The FTC also has participated in implementing bilateral interoperability programs such as the U.S./E.U. Safe Harbor Framework. Moreover, the FTC has promoted global privacy interoperability through various cross-border enforcement cooperation initiatives involving privacy enforcement authorities, such as the Global Privacy Enforcement Network (GPEN).

The draft regulation raises two significant obstacles to interoperability between the European privacy regime and the privacy regimes in the United States and other regions. First, it proposes divergence rather than convergence on several substantive issues. Second, its provisions on data transfers appear to create new obstacles to the flow of data across borders.

a. Divergence From Existing Standards

Many EU officials and privacy experts have for years stressed the value of seeking more global harmonization on privacy issues. As Richard Thomas, UK Information Commissioner, put it at the 2007 IAPP Summit: "Doing global privacy better means an active commitment to harmonization. Just as it is important that U.S. privacy laws are not discussed in isolation from the rest of the world, so too must the European Union be ready to consider changes." Indeed, recent multilateral efforts led by European data protection authorities to develop international consensus around common and internationally accepted privacy standards have been premised on the idea of increased harmonization between Europe and other countries and regions.[2] The draft regulation, however, proposes several far-reaching provisions that are inconsistent with many existing international or regional principles and standards. It widens, rather than narrows, the gap between different countries' practices."[3] Although some change and innovation in

[2] For example, many European data protection authorities supported the *International Standards on the Protection of Personal Data and Privacy* (the "Madrid Resolution") proposed by the Spanish Data Protection Authority at the International Conference of Data Protection and Privacy Commissioners held in Madrid on November 5, 2009. The resolution is available at http://www.privacyconference2011.org/htmls/adoptedResolutions/2009_Madrid/2009_M1.pdf. The FTC, which is now a member of the ICDPPC, attended the Madrid meeting as an observer, and FTC staff has pointed out the many challenges of such attempts at harmonization. *See Comments by the FTC staff and the DHS Privacy Office on the Joint Proposal for International Standards on the Protection of Privacy with regard to the Processing Of Personal Data* (the "Madrid Resolution") (August 10, 2010), available at http://www.ftc.gov/oia/consumer.shtm.

[3] *Cf. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), available at http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00.html.

substantive rules will of course be appropriate, there is value in thinking very carefully about dramatic changes that make interoperability on data practices even more difficult. Certain aspects of the draft regulation's treatment of issues such as data breach, children's privacy, and the newly proposed "right to be forgotten," for example, present significant hurdles to interoperability, which we discuss in more detail below.

i. Data Breach Requirements

The draft regulation sensibly proposes a general data breach notice requirement, applying uniformly across sectors and across the EU. This is in large measure consistent with the FTC's longstanding recommendation for a federal standard in the U.S. that covers the commercial sector generally.[4] Data breach notification requirements benefit consumers by raising public awareness of data security issues and related harms, as well as data security issues at specific companies. There is a concern, however, that certain of the requirements proposed may be so strict that they impose compliance costs passed on to consumers that far outweigh the benefits consumers might get from such requirements. A related concern is that an overly strict standard may, for compliance reasons, affect practices in the U.S. as well, especially for multi-national companies subject in some way to an EU member state's jurisdiction. Compliance with such provisions may harm U.S. consumer welfare by diverting attention away from core consumer privacy issues such as how to improve corporate data security practices.

The draft regulation's proposed data breach notification rules may pose such problems. In the case of a breach, the controller must notify a DPA "not later than 24 hours after the personal data breach has been established." Article 28(1). "Personal data breach" is defined broadly as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed." Article 3(9). Moreover, the notice must provide various details, such as the number of data subjects concerned, the number of data (sic) concerned, recommended and undertaken mitigation measures, and the consequences. And if the breach "is likely to adversely affect the protection of the personal data or privacy of the data subject," the controller must within that same 24 hours notify the data subject.

Experience with actual data breaches suggests that in many instances this process could be difficult, expensive, and even counterproductive. Suppose, for example, that a company discovers at 9:00 a.m. that it lost data on 17 million phone customers (*cf.* Deutsche Telekom), or may have lost laptops with 18 million health records (*cf.* UK NHS). By the beginning of the next business day, the company would have to determine what exactly had happened and identify how many individuals were affected. If the company determined that the Article 29 requirement

---

[4] *See Prepared Statement of the Federal Trade Commission on Privacy and Data Security: Protecting Consumers in the Modern World before the Committee on Commerce, Science, and Transportation, United States Senate,* Washington, D.C., June 29, 2011, at p. 2, available at http://www.ftc.gov/os/testimony/110629privacytestimonybrill.pdf.

applied, it would have to identify the individuals and send out millions of notices in a very short time frame, perhaps even before the company has accurate information about the data breach and the individuals affected to avoid a "fine between 100 000 EUR and 1 000 000 EUR or, in case of an enterprise up to 5 % of its annual worldwide turnover." This appears to be the case even if the company negligently but not intentionally, does not "timely or completely notify the data breach to the supervisory authority or to the data subject." Article 79(4)(h). The draft regulation thus makes it more likely that a company may err on the side of over-notification, resulting in a stream of notices that may wind up going to the wrong people or, even worse, make the company's systems (and the consumer data in them) more vulnerable by publicizing a breach before all of the vulnerabilities have been identified. Such a focus on process, instead of on improving security practices, may over time dilute the effectiveness and credibility of all such notices.

ii. "Right to be Forgotten"

In connection with a proposed "right to be forgotten," the draft regulation proposes a "right to obtain erasure of any public Internet link to, copy of, or replication of the personal data relating to the data subject contained in any publicly available communication service." Article 15(2), draft regulation at 9. (We note that this says "any" link, copy, or replication, not just those under the control of the controller who first processed the information.) While there are or may be exceptions when "necessary" in connection with freedom of expression, see Article 15, 79, and 80, the draft regulation sets forth strict penalties for both intentional and negligent failures to comply with this requirement.[5]

There are indeed important consumer privacy issues raised by the seemingly endless lifespan of information in the online world. But there is a serious question whether such an expansive version of a "right to be forgotten" is at all practical even within the EU.[6] Indeed, it is unclear how such a broad right would be feasible given that personal data is often posted widely in public places and re-shared by third parties, and that publicly available information can and does

[5] The draft regulation requires supervisory authorities to "impose a fine between 500 EUR and 600 000 EUR, or in case of an enterprise up to 3 % of its annual worldwide turnover," to anyone who "intentionally or negligently ... does not erase any public Internet link to, copy of, or replication of the personal data relating to the data subject contained in a publicly available communication service pursuant [to] Article 15." Article 79(3)(c).

[6] *See "Right to be forgotten may not be enforceable . . . We don't yet have a Men in Black flashy thing,"* available at http://www.theregister.co.uk/2011/11/15/right_to_be_forgotten_might_not_be_enforcable/.

flow across borders.[7] There is also a serious question as to how this newly created right squares with freedom of expression generally, and with U.S. freedom of speech rights in particular.[8] These examples show how the draft regulation may at least in certain circumstances impose restrictions upon business that may prove impractical and without corresponding consumer or public benefit.

iii. Definition of "Child"

The draft regulation commendably addresses the privacy of children, an issue of longstanding and increasing concern in the U.S. Indeed, the FTC recently reviewed the effect of its rule implementing the Children's Online Privacy Protection Act (COPPA), 15 U.S.C. 6501 *et. seq.*, which defines a "child" as an individual under the age of 13. 15 U.S.C. at 6502(1). Unlike the U.S. law and rule, the draft regulation defines "child" as "any person below the age of 18 years," Article 3(18), and provides that "Consent of a child shall only be valid when given or authorized by the child's parent or custodian." Article 7(6). Clearly there is a range of reasonable policy choices here. There is a question, however, whether requiring parental consent for all teenagers under 18, and treating them in the same way as small children in all contexts, is the most practical approach. As the FTC noted in its COPPA Rule review, it would be difficult to require parental permission for teenagers because they're independent, more sophisticated with new technologies than their parents are, and have access to computers outside the home, particularly with the increasing proliferation of mobile devices. There is also a serious question whether it is advisable or feasible to define children so broadly, not just for practical reasons, but also because of older children's own rights, as they age, to access information and express themselves publicly.[9]

---

[7] Compare the case of "Tron," the name used by a German hacker. It was reported that after his death, his parents sued to keep his real name off the Wikipedia.de website, and temporarily obtained an injunction. http://www.spiegel.de/international/0,1518,396307,00.html . But this did not remove the information from Wikipedia's U.S. website. And an academic researcher's "small experiment" showed that the number of related searches for his real name actually increased after the injunction, suggesting "that there is no (legal) remedy available that could prevent such a thing from happening – this is of course due to the decentralized, multijurisdictional character of the Web." *See* http://blogs.law.harvard.edu/ugasser/2006/02/10/figures-tell-hacker-tron-more-popular-than-ever-after-restraining-o/

[8] Consider, for example, the case of the German murderers suing Wikipedia to remove references to their names or the case of the Spanish DPA pursuing a search engine for not deleting from its search results information from such public sources as a Spanish government website entry or a news article. *See* http://www.wired.com/threatlevel/2009/11/wikipedia_murder/ and http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202491072664&slreturn=1. It would appear unlikely that such cases could be pursued in the U.S.

[9] *COPPA Rule Review Request for Comment*, Fed. Reg. Vol. 76, No. 187, Sept. 27, 2011 at 5905, available at http://ftc.gov/os/2011/09/110915coppa.pdf.

b. Provisions Governing Transfers to Third Countries

i. Adequacy Determinations

The European Commission earlier indicated that it intended, in its draft proposal, to "clarify the Commission's adequacy procedure and better specify the criteria and requirements for assessing the level of data protection in a third country or an international organization."[10] Indeed, DG Justice Commissioner Reding has been quoted as stating that "Clear rules are needed for the transfer of data outside the EU."[11] Yet it appears that is not what the draft provides.

The initial communication from the European Commission that led to the draft regulation identified certain difficulties with "adequacy," including the lack of harmonization among the member states. Although the lack of harmonization within the EU may indeed be a challenge, there are additional significant shortcomings in the "adequacy" framework for third countries, such as the lack of transparency and clarity in the procedure and the cumbersome nature of the process."[12] Indeed, there have only been a handful of adequacy determinations since 1995. The new provisions in the draft regulation are unlikely to make these determinations any easier.

The draft regulation will only increase the complexity by now adding laws concerning "public security, defense, national security and criminal law as well as the professional rules and security measures which are complied with in that country . . ." to the laws that need to be considered in an "adequacy" determination. Article 38(2)(a). In considering the "adequacy" process, a telling point of comparison is the recent European Court of Justice decision in Akzo Nobel on attorney-client privilege. There the ECJ's advocate general suggested it would "not even be possible" and would impose "considerable expense" to evaluate the propriety of applying attorney-client privilege in other countries."[13] The current data protection directive evaluates the "adequacy" of a country's entire privacy regime "assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations," with particular consideration for "the

---

[10] *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions regarding "A comprehensive approach on personal data protection in the European Union,, Brussels, 4.11.2010 COM (2010) 609 final at 16.*

[11] Viviane Reding, *The Future of Data Protection and Transatlantic Cooperation* (Speech at the 2nd Annual European Data Protection and Privacy Conference Brussels) (Dec. 6, 2011), available at http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/851&format=HTML&aged=0&language=EN&guiLanguage=en.

[12] *FTC Staff comments on the European Commission's November 2010 Communication on Personal Data Protection in the European Union* at 8, January 13, 2011, available at http://www.ftc.gov/os/2011/01/111301dataprotectframework.pdf.

[13] *Introductory Note to the European Court Of Justice: The Akzo Nobel EU Attorney-Client Privilege Case,*" By Laurel S. Terry, September 14, 2010, 50 ILM xxx (2011), available at http://www.asil.org/infocus100914.cfm.

nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country." Art. 25. To the extent the draft regulation provides for an even broader array of legislation than that considered currently by the Article 29 and 31 committees, the draft regulation only makes the process more burdensome, opaque, and indeterminate. In the past 15 years, only a handful of such determinations have been made, and it is unclear how, when, or why any such determinations might ever be changed.

ii. Alternative Provisions for Data Transfer

To achieve global interoperability, regulators have been exploring the use of codes of conduct, privacy certification schemes, seals and trustmarks to facilitate cross-border data transfers while ensuring privacy protections for consumer's personal data. The APEC Cross-Border Privacy Rules project is one example of such a scheme. EU data protection authorities have also championed the further development of such mechanisms.

It is unclear to what extent the draft regulation is consistent with such developments. Article 35 of the proposed regulation appears to encourage the use of codes of conduct, including for transfers to third countries, while Article 36 provides for trustmarks, seals, and other data protection certification mechanisms, and vests the European Commission with powers for "requirements of recognition within the Union and third countries." From a simple reading of the text, however, it is not clear whether the codes of conduct referred to in Article 35, or the certification mechanisms, seals and marks referred to in Article 36, are intended to be used as interoperability mechanisms for cross-border data transfers between the EU and third countries.

Such an interpretation of these articles also appears to conflict with the immediately following provisions in Chapter V concerning the transfer of personal data to third countries, in which the use of codes of conduct and the certification mechanisms, seals and marks are not mentioned as a vehicle for data transfers to third countries. The list of criteria for adequacy does not now expressly include "adequacy" findings with respect to specific industry codes of conduct, and other certification schemes, privacy seals and marks that could be developed for or by specific "processing sectors" or other industry groups. Including this option would go a long way towards enhancing interoperability with third countries.

2. Regulatory Enforcement and International Cooperation

The draft regulation raises three major concerns affecting both regulatory enforcement in general and international enforcement cooperation in particular.

a. The draft regulation appears to interfere in dramatic fashion with the domestic investigations of third countries' public agencies, such as the FTC. Article 42(2), which essentially takes the form of a "blocking statute," provides that where a court or administrative authority "requests" a controller to disclose personal data, the controller must notify a data protection authority, and "must obtain prior authorization for the transfer . . . ." (We assume that the term "requests" refers to orders, subpoenas, and requests made for voluntary production where the alternative is

mandatory production.) The preamble to the draft regulation (at 74) similarly states that "provision should be made to prohibit a controller or processor to directly dispose personal data to requesting third countries, unless authorized to do so by a supervisory authority [*e.g.*, a member state data protection authority]. The explanatory memorandum suggests, without further explanation, that this is intended to apply to a controller "operating in the EU."

Others will highlight the conflicts and perils this creates for companies with an EU presence that are involved in private U.S. litigation.[14] This note will focus only on the critical enforcement impediment that the draft regulation appears to pose to U.S. agencies charged with protecting the public interest. In short, the draft regulation appears to impede the ability of a public regulatory agency like the FTC to access information necessary for an investigation, and to hinder the ability of U.S. regulatory enforcement agencies to cooperate with their EU member state counterparts.

Suppose, for example, that the FTC (or the SEC, the CFTC, the CPSC, or any number of other agencies charged with protecting the public) voluntarily requests or subpoenas documents from a U.S. company or from a European company doing business in the U.S. in an investigation. The investigation might involve mergers, anti-competitive activities, financial or consumer fraud, safety risks, or even privacy violations -- activities that could affect scores of Americans (and in some cases Europeans). As drafted, the proposed regulation creates incentives for such firms to avoid the request or subpoena by "offshoring" evidence, thereby hindering the U.S. investigation and leading U.S. agencies to pursue otherwise unnecessary court challenges. In addition, it is unclear what the relevant supervisory authority would be expected to do as part of its review; is a DPA, for example, expected to decide what evidence the FTC needs to investigate a malicious spyware case, and how important that case is to protecting U.S. consumers?

What is clear is that such a system would, at the very least, introduce delay, particularly damaging to Internet-related investigations and merger reviews, where time is of the essence. To avoid sanction under Article 42 of the draft, the firm from which information is requested either would have to make a request for authorization to the data protection agency or go through the time-consuming task of redacting relevant personally identifiable information from any documents submitted. This might include names, titles, and addresses and other personal information. Under either approach, the FTC would find it difficult or impossible to use such information in a reasonable timeframe, such as the timelines mandated for merger reviews.

Moreover, the production of documents redacted of all personal information is likely to render much of the information useless to U.S. investigators. For example, in an antitrust review, the FTC would be unable to identify whether the document's drafter, the identity of which would be redacted, was authorized to speak on the firm's behalf. This would not only deny U.S. agencies such as the FTC effective access to the information needed for its own investigations, but also

---

[14] *Cf. Societe Nationale Industrielle Aerospatiale et al. v. U.S. Dist. Ct. for the So. Dist. of Iowa*, 482 U.S. 522 (1987).

impede an agencies' ability to cooperate with its EU and member state counterparts on matters that they were jointly investigating. Accordingly, the draft regulation would effectively undermine international cooperation. This could be particularly problematic when cooperation laws condition enforcement cooperation on reciprocal assistance.[15]

b. The draft regulation also does not clearly permit transfers from regulatory enforcement agencies in the EU or its member states to third country agencies such as the FTC. Indeed, given the current reading of various provisions in the 1995 Data Protection Directive, it appears that the approach may be the opposite. Currently, at least certain European Commission directorate-generals take the view that they are limited or precluded in exchanging information directly with their counterparts in the U.S. government in enforcement matters absent extensive negotiations demanding large-scale incorporation of "adequacy" standards that in our experience are not required even of the EU's own enforcement agencies. There is a concern that the adoption of the new package will crystalize this view, and limit the ability of EU and member state agencies to exchange covered information with the FTC, again severely impacting transatlantic cooperation.

c. The draft regulation commendably provides for international cooperation mechanisms for the protection of personal data, taking into account the 2007 OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy. However, it appears that the draft limits full cooperation to countries deemed "adequate." This would focus cooperation where it's easy bureaucratically, not necessarily where it's most needed. The reality is that the EU member states have in the past, and will in the future, authorize transfers to countries all over the world, with a variety of standards, and that an enforcement system that isn't global in focus isn't "adequate" to the task.

Finally, the term "supervisory authority" in connection with international cooperation excludes privacy enforcement authorities that are differently organized and structured than "supervisory authorities" under the European model. It is unclear why the draft regulation does not use "privacy enforcement authority" as it is defined in the 2007 OECD Recommendation on Cross-border Co-operation that the draft regulation takes into account. ("Privacy Enforcement Authority" means any public body . . . that is responsible for enforcing Laws Protecting Privacy, and that has powers to conduct investigations or pursue enforcement proceedings"; *see also* OECD definition of "Laws Protecting Privacy"). Essentially, that definition would capture any public authority that has the authority to conduct investigations and enforcement proceedings under national privacy laws and thus would be more appropriate and productive for purposes of international cooperation.

It is hoped you find these comments useful as you further consider the revisions to the EU's data protection directive. Thank you for considering them.

---

[15] See *U.S. SAFE WEB Act of 2006, 15U.S.C. 46(j)(3)(A)* (authorizing FTC to provide investigative assistance to foreign law enforcement authorities in appropriate cases and circumstances when the foreign agency "has agreed to provide or will provide reciprocal assistance to the Commission).