KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

COMMENTS OF THE CENTER FOR DEMOCRACY & TECHNOLOGY

TO THE EUROPEAN COMMISSION

IN THE MATTER OF

CONSULTATION ON THE COMMISSION'S COMPREHENSIVE APPROACH ON PERSONAL DATA PROTECTION IN THE EUROPEAN UNION

January 15, 2011

Introduction

The Center for Democracy & Technology (CDT) is pleased to offer this contribution to the Commission's consultation on Directive 95/46/EC. We hope that these comments, which draw upon CDT's research and advocacy, will assist the Commission in addressing the challenges posed by new technologies and business practices and by the reality of global data flows.

In these comments, we provide suggestions for strengthening the core principles of the Data Protection Directive (DPD) and for more rigorously implementing those principles across the European Union. We also discuss the intersection of the Data Protection Directive with other fundamental interests such as innovation and free speech.

About CDT

CDT is a non-profit, non-governmental public interest organization with offices in Washington, DC and San Francisco, CA. Our mission is to keep the Internet open, innovative and free. We accomplish our mission through technical, policy and legal analysis, consultation with industry, academia and other stakeholders, and advocacy. Since our establishment in 1994, CDT has helped to shape public policy on a wide range of Internet issues, including consumer privacy. For example, CDT created the Anti-Spyware Coalition, which helped to build consensus definitions and best practices for anti-spyware products. In addition to a Project on Consumer Privacy, we also have a dedicated Project on Health Privacy and recently added a Project on Global Internet Freedom. CDT advocates in the United States for adoption of a comprehensive federal consumer privacy law based on a full set of Fair Information Practices, combined

with robust industry practices and privacy by design. CDT coordinates the Internet Privacy Working Group, a forum for consumer advocates and Internet companies, where stakeholders engage in dialogue and seek consensus on consumer privacy issues. We have worked with industry on privacy best practices (for example on the use of RFID), and we offer consumers a wide range of educational resources. CDT staff testify regularly before Congressional committees and present frequently before governmental agencies and technical standards bodies. Last year, we submitted comments[1] to the Commission's Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data. For the past year, we have been deeply engaged in consultations – still ongoing -- before the U.S. Department of Commerce and the U.S. Federal Trade Commission, both of which are revisiting the policy framework for consumer privacy in the U.S. and confronting many of the same issues raised by the Commission in this consultation.

Strengthening Key Principles of the Directive

The Commission has posed many questions around how to strengthen the core principles of Directive 95/46/EC. Below we address the Commission's questions through recommendations that emphasize ways to strengthen the transparency, control, data minimization, and accountability principles.

Increasing Transparency for Data Subjects

Simplification and standardization of privacy notices

The Commission has sought comment on whether it should draw up one or more EU standard forms ('privacy information notices') to be used by data controllers. The feasibility of standard privacy notices is presently also a hot topic in the United States, and the discussions and analyses in the U.S. may be of value to the Commission at it considers these issues. The Federal Trade Commission (FTC) has concluded that traditional privacy policies, written in complicated and legalistic language, are not a sufficient form of notice; accordingly, the FTC is reexamining its standards for notice and has suggested that there may be a role for standardized "short form" privacy notices.[2] The FTC has suggested in its December 2010 privacy report, which is currently open for comment, that notice should be provided in a clear, concise, comparable, and time-appropriate manner.[3] This means notices should be easy for the average person to understand, presented in a few short sentences, placed in a sensible

[1] Comments of the Center for Democracy & Technology, in the Matter of Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data (Dec. 31, 2009), *available at* http://www.cdt.org/files/pdfs/CDT%20Comments%20to%20the%20European%20Commission.pdf.

[2] Federal Trade Commission (Bureau of Consumer Protection), *A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, 57-63 (Dec. 1, 2010) *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

[3] *Id.*

location, written in a format such that individuals can compare across websites, and displayed at a time relevant to the consent.[4]
Coordination between U.S. and EU privacy regulators on what a standardized privacy notice might look like would certainly be fruitful. Consumers and companies alike would benefit from an Internet in which companies can comply with the notice requirements of both the U.S. and the EU with just one notice and individuals can compare and contrast the privacy practices of European and U.S. companies.

Notice of data breaches would promote transparency and accountability

The Commission has sought comment on whether the principle of transparency can be strengthened through the adoption of a personal data breach notification requirement similar to that found in the E-Privacy Directive (which only applies to the telecom sector). Based on the experience in the U.S., where most states have adopted breach notification statutes, resulting, in effect, in a national breach notification requirement, we believe that data breach notification requirements promote corporate transparency and accountability and encourage the adoption by companies of stronger data security protections.

The data breach notification provisions of the amended E-Privacy Directive[5] could serve as a useful starting point for development of a general EU breach notification standard. In particular, CDT supports retaining the provision of the E-Privacy Directive that exempts companies from notifying individuals of data breaches when "the provider has demonstrated to the satisfaction of the competent authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the security breach."[6] A similar standard has been adopted by many states in the U.S. and seems not to have impeded the effectiveness of the breach notification concept.

CDT urges the Commission, however, to refrain from extending without modification two of the provisions of the E-Privacy Directive's data breach notification requirement. First, the E-Privacy Directive requires notification only if the company affirmatively finds that there has been a breach of personal data whose release will have an adverse affect on individuals. This standard effectively disincentivizes a company from investigating potential breaches; a company that has suffered a breach may not want to examine the circumstances around the breach too closely, because finding evidence of risk would trigger the obligation to notify. Hence, CDT recommends that any extension of a data breach notification requirement include a "notify unless" formulation: companies should be required to notify individuals of a breach of their personal data *unless* it can be determined that the data breach is not likely to affect an individual to a degree that triggers notification. Such a formulation will encourage companies to carefully investigate all breaches.

---

[4] Many of these principles had also been recognized previously by the Federal Trade Commission (FTC) in the United States. *See In re* Sears Holdings Mgmt. Corp., Docket No. C-4262 (Aug. 31, 2009) (Decision and Order) *available at* http://www.ftc.gov/os/caselist/0823099/090604searsdo.pdf (FTC ordered that "the required disclosures [must be] of a type, size, and location sufficiently noticeable for an ordinary consumer to read and comprehend them, in print that contrasts with the background on which they appear" and "on a separate screen from, any final 'end user license agreement,' 'privacy policy,' 'terms of use' page, or similar document.").

[5] *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector*, *as amended by* Directive 2009/136/EC, Article 4(3).

[6] *Id.*

CDT also urges the Commission to reconsider its decision that notification is required only if harm is likely (the "adverse effects" test). The guidance presented by the recitals to the amended E-Commerce Directive suggests that "[a] breach should be considered as adversely affecting the data or privacy of a subscriber or individual where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation in connection with the provision of publicly available communications services in the Community." "Significant" humiliation or damage to reputation could be interpreted as a very high standard for notification.[7] It does not recognize that breach of sensitive information – such as health or financial information – should always trigger a notice, and it may encourage companies to avoid notification by minimizing their interpretation of the "adverse effect" of breaches. While the E-Privacy Directive empowers the competent national authority to effectively reverse such a determination (and we would encourage any extension of the data breach notification requirement to include similar override powers), the resources available to such authorities to follow up on these decisions are typically small.

In the United States, many of the state-level data breach notification laws have rejected the harm standard.[8] And in 2005, attorneys general from 45 states, the District of Columbia, and Puerto Rico signed a letter to the U.S. Congress, which at the time was considering a harm standard. The letter stated:

> "We also believe that the standard for notification should be tied to whether personal information, whether in electronic or paper form, was, or is reasonably believed to have been acquired or accessed by an unauthorized person, rather than a standard that includes an additional requirement that the breach entail actual harm or a measure of risk of harm. Standards that require additional proof by a tie to harm or to a risk of harm place the bar too high. It is extremely difficult in most cases for a breached entity to know if personal data that has been acquired from it by an unauthorized person will be used to commit identity theft or other forms of fraud."[9]

Some companies may claim that a harm standard ensures that consumers are not overwhelmed by unnecessary notices. However this argument incorrectly presupposes that the only purpose of breach notification is informing individuals of the steps they can take to protect themselves from the consequences of the breach. While this is in fact one purpose behind breach notification standards, it ignores the larger goal of the policy: reducing the number of data breaches by incentivizing companies to improve their data security practices. Indeed, a 2007 study of the impact of state-implemented breach laws conducted by the Samuelson Law, Technology, & Public Policy Clinic at the University of California, Berkeley found that "regardless of the risk of identity theft and alleged individual apathy towards notices, the simple fact of

---

[7] Directive 2009/136/EC of 25 November 2009, Recital 61.

[8] Among these states are four of the five most populous: California, Illinois, New York, and Texas. Combined, these states make up more than thirty percent of the United States population, with California alone comprising more than one-tenth of the population. Any entity doing business with these states or on a nationwide basis must comply with the laws of these states. *See* e.g., Cal. Civ. Code § 1798.82, 815 Ill. Comp. Stat. § 530/10, NY Gen. Bus. Law § 899-aa, and Tex. Bus. & Com. Code § 48.103.

[9] Letter from the National Association of Attorneys General to Honorable Bill Frist et. al (Nov. 7, 2005) *available at* http://www.cdt.org/security/State_AGs_2005_Letter_to_Congress_on_Breach_Notification.pdf.

having to publicly notify causes organizations to implement stronger security standards that protect personal information."[10]

Strengthening Consent: Improving Mechanisms for Obtaining Consent after a Material Change to Data Collection and Use Practices

The Commission seeks comment on how to strengthen the rules on consent. One area that deserves attention is the consent needed when the data collector makes a material change to its data collection or use practices. The question of how to obtain consent from data subjects for this material change has challenged companies and consumer advocates alike. A notice on the webpage that hosts the privacy policy is clearly insufficient – but what would be sufficient?

One promising approach involves presenting a user with a "forced choice" that compels meaningful participation before a material change can take effect. For example, in offering Pandora users the option to share their music listening habits through Facebook, Pandora's webpage prompts users to choose whether they want their profile to be "public" or "private." Users must choose one or the other — they cannot simply close the box. The box also contains links to information that gives users the chance to learn more about sharing works. This method prevents users from unwittingly bypassing important decisions.[11] While a forced choice is not desirable for all data practices requiring consent, we believe it is appropriate for material changes to data collection or use practices.

The Data Retention Directive Is an Obstacle to Efforts to Strengthen the Principle of Data Minimization

In considering how to strengthen the principle of data minimization, the Commission should consider the impact of Directive 2006/24/EC, the Data Retention Directive. [12]

The Commission, of course, has a separate proceeding to examine the Data Retention Directive. If, as a result of that inquiry, the Commission does not repeal or substantially narrow the Data Retention Directive, it should consider limiting companies from using for commercial

---

[10] Samuelson Law, Technology, & Public Policy Clinic, *Security Breach Notification Laws: Views from Chief Security Officers*, University of California-Berkeley School of Law (2007). The study found: "Breach notification laws have significantly contributed to heightened awareness of the importance of information security throughout all levels of a business organization and to development of a level of cooperation among different departments within an organization that resulted from the need to monitor data access for the purposes of detecting, investigating, and reporting breaches. [Chief Security Officers] reported that breach notification duties empowered them to implement new access controls, auditing measures, and encryption. Aside from the organization's own efforts at complying with notification laws, reports of breaches at other organizations help information officers maintain that sense of awareness."

[11] *See* Justin Brookman, *Closing Pandora's Box*, CDT Blog, August 4, 2010 *available at* http://www.cdt.org/blogs/justin-brookman/closing-pandora's-box.

[12] *See* Cecilia Malmström, Member of the European Commission responsible for Home Affairs, *Taking on the Data Retention Directive* (Dec. 3, 2010) *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/723. As the Commission is well aware, the national constitutional courts that have taken up the Directive have either rejected it or rejected their particular nation's transposition. In addition, it is clear that the Directive has had a negative impact on citizens' willingness to access information. *See* European Digital Rights, *What the European Commission owes 500 million Europeans*, Dec. 3, 2010 *available at* http://www.edri.org/files/Data_Retention_Conference_031210final.pdf.

purposes the IP addresses, location information, and other personal or personally identifying data they have retained as a result of its implementation.

Strengthening the Principle of Accountability

Accountability has various elements, and there is growing recognition of the importance of creating accountability structures for all stages of the process by which businesses (and government agencies) conceptualize, design, launch and maintain products and services that process personal data. One such accountability structure is an obligation for data controllers to carry out a data protection impact assessment (or "privacy impact assessment" or PIA) prior to the launch of any new products, services or marketing initiatives that involve the collection, use, or disclosure of covered data. In the U.S., a federal law requires federal agencies to conduct such assessments, and a growing number of companies have voluntarily adopted the practice. Such assessments, conducted during the planning stages of a product or service and then updated as the product or service develops, should link the nature and amount of data collected to the purpose for which it will be used. They should also explore protocols for storing, transferring, and deleting data. Such assessments serve to identify privacy issues at an early stage, so that steps can be taken to minimize them while the product or service is still being developed. [13]

Another accountability mechanisms where the United States has shown leadership has been in the appointment of "Chief Privacy Officers" and the creation of internal privacy compliance infrastructures. Again, as a matter of U.S. federal law, all federal agencies must appoint Chief Privacy Officers, and most major companies have voluntarily chosen to appoint such officers, who develop rules and practices and internally monitor compliance with applicable laws.[14] The Commission should consider whether adding an accountability principle to the Directive could foster better internal decision-making about the processing of individuals' data.

Some of these new principles and mechanisms for integrating privacy considerations into business models and product development cycles are referred to as "Privacy by Design." The concept has been prominently championed by Ann Cavoukian, Ontario's Information and Privacy Commissioner, and was endorsed by the Privacy Commissioners at their recent meeting in Israel.[15] The concept encourages companies to take responsibility for data processing by inculcating a culture of privacy throughout their organizations.[16] The Commission should explore ways to incentivize companies to implement "Privacy by Design" into the development of their offerings.

---

[13] For more information on how accountability measures can be incorporated into the product development cycle *see* Marty Abrams, Ann Cavoukian, and Scott Taylor, *Privacy by Design: Essential for Organizational Accountability and Strong Business Practices* (Nov. 2007), *available at* http://www.ipc.on.ca/images/Resources/pbdaccountability_HP_CIPL.pdf.

[14] *See* Kenneth A. Bamberger and Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 Stan. L. Rev. (forthcoming 2011) *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1568385.

[15] *See* Privacy: Generations, *"Privacy: Generations", the 32nd International Conference of Data Protection and Privacy Commissioners closes with a new executive committee and new members* (accessed Jan. 14, 2011) *available at* http://www.privacyconference2010.org/news_view.asp?id=24.

[16] For more information, see Ann Cavoukian, Privacy by Design: The 7 Foundational Principles (August, 2009), available at http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf.

Implementation of the Directive

Improved Enforcement

One of the most needed improvements to the EU's privacy protection framework is also perhaps the most straight-forward: the allocation of more resources toward enforcement of the Directive. Despite the very strong top-level principles embodied in the Directive, uneven and vague implementation at the member state level and limited enforcement have given companies inadequate guidance in developing their privacy practices and left consumers unprotected against new and potentially unfair processing of their personal data.[17] While the biggest industry players may come under scrutiny,[18] many smaller actors can fly under the radar and avoid accountability for bad practices. This problem is particularly serious in a world where mobile "apps" distributed by very small companies can easily gain access to tremendous amounts of personal data.[19]

To be clear, lax enforcement is not unique to Europe. In the United States, CDT has repeatedly called on the Federal Trade Commission[20] and state Attorneys General[21] to more aggressively use their investigatory and enforcement powers to bring both clarity and accountability to companies that process personal data.

One way to improve enforcement may be through cooperation among multiple countries' Data Protection Authorities on joint investigations. In the United States, multi-state investigations and joint enforcement proceedings by state Attorneys General have produced important successes, including cases against companies installing "spyware" on individuals' computers,[22] against social networking sites,[23] and an ongoing investigation into deceptive financial account information transfers.[24]

An increased emphasis on enforcement does not necessarily mean, of course, that companies should be absolved on their *ex ante* notification obligations under Article 18. To the contrary,

---

[17] Seven years ago, a Commission Report noted that state "supervisory authorities [held] a wide range of tasks, among which enforcement actions have a rather low priority." First implementation report of the European Commission on the Data Protection Directive (May 15, 2003) *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52003DC0265:EN:HTML.

[18] *See*, *e.g.*, Kevin J. O'Brien, *Europe Pushes Google to Turn Over Wi-Fi Data*, N.Y. TIMES, June 27, 2010, *available at* http://www.nytimes.com/2010/06/28/technology/28google.html; *Facebook "Not Abiding by Law" in Europe*, CBS NEWS, March 25, 2010, *available at* http://www.cbsnews.com/stories/2010/03/25/tech/main6331208.shtml.

[19] *See, e.g.,* Spencer Ante, *Google Disables Android Apps Caught Collecting Personal Data*, THE WALL STREET JOURNAL, Digits Blog, July 29, 2010, *available at* http://blogs.wsj.com/digits/2010/07/29/android-wallpaper-apps-caught-collecting-personal-data/.

[20] *See* Comments for Center for Democracy & Technology, *In re* FTC Consumer Privacy Roundtable (Nov. 6, 2009), *available at* http://www.cdt.org/files/pdfs/20091105_ftc_priv_comments.pdf.

[21] *See* Reece Rushing et al., *Online Consumers at Risk and the Role of State Attorneys General* (Aug. 2008), *available at* http://www.americanprogress.org/issues/2008/07/pdf/consumer_protection.pdf.

[22] Robert McMillan, *Sony Rootkit Settlement Reaches $5.75M*, PCWORLD, December 22, 2006, *available at* http://www.pcworld.com/article/128310/sony_rootkit_settlement_reaches_575m.html.

[23] Proskauer Privacy Law Blog, *State Attorneys General Announce Agreement with MySpace to Protect Children Online*, Jan. 15, 2008 *available at* http://privacylaw.proskauer.com/2008/01/articles/childrens-online-privacy-prote/state-attorneys-general-announce-agreement-with-myspace-to-protect-children-online/.

[24] Greg Sandoval, *Mr. President, please protect Web shoppers*, CNET NEWS, Dec. 20, 2010 *available at* http://news.cnet.com/8301-31001_3-20026152-261.html.

clear and meaningful specification of the purposes for which they are collecting and processing personal data is fundamental to individuals' ability to make informed choices about their data, and companies should be focused on delivering more clear and transparent notices both to regulators and individuals than they currently are. However, complying with disparate approaches to Article 18 adds complexity and administrative cost to companies without adding privacy protection benefits to consumers. The Commission should explore ways to allow for companies to accomplish their notification obligations in a consolidated manner.

Coregulation

One of the fundamental challenges in developing and implementing a privacy protection framework is to provide flexibility while also establishing comprehensive and firm rules. Given the disparity among sectors and the differences between online and offline business and between small and multinational enterprises, a one-size-fits-all approach that narrowly prescribes all data practices is likely to unfairly favor certain companies while stifling innovation and development by others.

Coregulation offers considerable promise as a means to offer flexible but effective privacy protections. A carefully crafted coregulatory program could give industries and industry segments flexibility to work with regulators to develop tailored privacy solutions that are consistent will the principles in a framework law while empowering regulators to enforce these industry standards. A coregulatory approach could accommodate differences between industries, create certainty for companies (because following approved practices would be deemed compliance with the baseline privacy statute), encourage privacy innovation over time, and reward the adoption of accountable practices.

As the U.S. experience has shown, pure self-regulatory approaches are insufficient.[25] In order to ensure meaningful protection, the coregulatory approach includes three key concepts: (1) law must specify the core elements of a privacy protection framework that all industry programs would have to address: (2) any industry program must be approved by the governmental regulator; and (3) the government regulator would have the power to enforce the agreed-upon standard.

The idea of coregulation, which is already integral to the Data Protection Directive under Article 27, is gaining favor in the United States. Last year, Congressman Bobby Rush introduced a baseline privacy bill that relied heavily on coregulatory "choice programs" to develop industry-specific rules on data processing.[26] CDT testified before the House Subcommittee on Commerce, Trade, and Consumer Protection in support of that bill, and specifically noted that the choice program approach was an innovative way to achieve strong but flexible privacy

[25] *See FTC Staff Report*, *supra* note 1. *See also* Ira Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, I/S: A Journal of Law and Policy for the Information Society (forthcoming 2011), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1510275.

[26] BEST PRACTICES Act, H.R. 5777, 111th Cong. (2009).

protections for individuals.[27] Last month, the United States Department of Commerce issued a "green paper" advocating a similar multi-stakeholder approach to privacy governance.[28]

To the extent that one of goals of this consultation is international harmonization, encouraging coregulatory approaches to privacy governance in Europe could also help promote greater global consistency as those industry standards could be adopted internationally. The Commission should seek ways to standardize approval of codes of conduct across the European Union in an effort to reduce unnecessary administrative burden and increase harmonization.

Europe may be well positioned for a coregulatory approach since the Directive already specifies the elements of a comprehensive privacy framework. In Europe, the coregulatory approach could potentially afford the needed industry-specific clarity and guidance that have heretofore been lacking under the Data Protection Directive. A coregulatory approach may also help Europe overcome one of the major problems with its current system, which is the difficulty of achieving EU-wide approval of binding corporate rules and standard contract clauses. Instead of individual companies having to seek approval of each Data Protection Authority, industry sectors and other industry groupings could take on that process.

In order to function, however, any coregulatory program needs to offer appropriate incentives to convince industry to participate in such a program. In the United States, some of the incentives that have been suggested to encourage coregulatory participation include deemed compliance with the law, immunity from private right of action, and opt-out permission (as opposed to affirmative opt-in) for the transfer of some data to third parties.[29]

Harmonization and Coordination

In other sections of these comments, we discuss the benefits of harmonizing and coordinating EU-wide approaches to enforcement, notification, and codes of conduct. The Commission should also explore ways in order to create increased harmonization of member states' substantive law as well. The Data Protection Directive was originally created in order to move member nations to a more common framework for data processing.[30] The need for such a common approach has increased markedly in the past fifteen years, as the world has become more interconnected and individuals have a much greater ability to interact with other individuals and companies in other countries.

The Commission should devise a way to harmonize member nations' approach to Binding Corporate Rules as a privacy-protective mechanism to enable multinational corporations to move data among non-EEA countries. Currently, even the best meaning of companies that have excellent protections in place cannot move data efficiently without subjecting itself to separate administrative processes in all EU countries. Such unnecessary restrictions on the

---

[27] Testimony of Leslie Harris before the House Subcommittee on Commerce, Trade, and Consumer Protection, July 22, 2010 *available at* http://www.cdt.org/testimony/testimony-leslie-harris-house-subcommittee-commerce-trade-and-consumer-protection.

[28] The Department of Commerce (Internet Policy Task Force), *Commercial Data Privacy and Innovation in the Internet Economy: a Dynamic Policy Framework* (Dec. 2010) *available at* http://www.ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf.

[29] *See* BEST PRACTICES Act, H.R. 5777, 111th Cong. (2009); *see also* Rubinstein, *supra* note 26.

free flow of data do not benefit individuals in any way, and to the contrary place arbitrary limitations on the ability of companies to offer computer processing services to their customers. CDT strongly agrees with the principle put forward in the Consultation that "[a]dministrative simplification should not lead to an overall reduction of the data controllers' responsibility in ensuring effective data protection" ; administrative simplification, by promoting more efficient resource allocation, is certainly consistent with more – not less – effect data protection.

The Data Protection Directive in a Web 2.0 World: The Complex Interaction of the Data Protection Directive, Privacy Rights, and Other Fundamental Rights

Modern communication on the Internet creates complexities that will make a "Right to be Forgotten" difficult to implement

The Commission has sought clarification on the so-called "right to be forgotten." This "right" involves a balance of competing values: the right of free expression among and about individuals against the rights to privacy and dignity. Europe and the United States take different approaches to reconciling this tension.[31] In the U.S., freedom of speech under the First Amendment of the Constitution takes generally takes precedence, while Europeans typically give countervailing weight to the privacy rights in ECHR Article 8 and other sources.

CDT subscribes to the more potent American articulation of the freedom of expression standard online and would strongly resist certain elements of a "right to be forgotten" if they were proposed in the US. However, recognizing this philosophical division, we urge the Commission to consider the practical implications a "right to be forgotten" might have in the online context. In short, any "right to be forgotten" should be crafted so as not to stifle social innovation, unravel the fabric of communication online, or overburden information intermediaries. The complexity of information flows online make a robust, practical "right to be forgotten" difficult to envision. However, a limited articulation of the right may be feasible.

Any "right to be forgotten" scheme must clearly distinguish between two kinds of data sharing and the related privacy concerns they raise: passive or transactional data sharing – when a service collects and uses personal data in the context of a commercial transaction, and active or expressive data sharing – when content is authored or disseminated by users themselves (for example, on a social network or user-generated content (UGC) hosting service).

The right to be forgotten has relevance in both contexts, but should be defined quite differently. In the context of passive data sharing, the "right to be forgotten" is to some extent already recognized in the U.S., although it is discussed in terms of limitations on data retention and use. For example, the U.S. Fair Credit Reporting Act places limits (quite long ones, to be sure) on the use in credit reports of bankruptcies that occurred years ago. To take another example, CDT has successfully urged search engines to reduce their retention of search logs, and we have supported efforts in the U.S. to empower individuals to access and challenge the accuracy of personal information that a data controller or data processer has collected or holds. Similarly, CDT supports requiring entities in the behavioral advertising industry, among others, to allow

[31] Franz Werro, *The Right to Inform v. The Right to be Forgotten: A Transatlantic Clash*, HAFTUNGSRECHT IM DRITTEN MILLENNIUM, 285-300 (May 2009), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1401357.

individuals to access, edit, and delete or block the use of the personal information that these companies hold about them.

Defining and applying a "right to be forgotten" in the context of active data sharing poses different complexities. CDT generally supports empowering individuals to delete data they themselves have created and stored with a third-party service. For example, a blogger should be able to remove her blog at any time. Similarly, an individual should have the option to delete her social networking profile and feel confident that the company that owns the social networking platform has not retained a copy of that profile. In both of these examples, a straightforward two-way relationship exists and a "right to be forgotten" is reasonably easy to define and implement. If a data subject decides to store data in the "cloud," she should be able to remove that data from the cloud as well.

However, CDT cautions that modern communication on the Internet creates complexities that will make a broader "right to be forgotten" difficult to implement. For example, while an individual should be able to delete her blog, she should not be able to delete comments on other websites that point to her blog or discuss her blog. Online communication is often intermingled, republished, and recast in a variety of contexts. For example, on Twitter, many users will "retweet" or recopy others' communications (with attribution and sometimes their own commentary) to their own account. Social networks, blogs, aggregation engines, and even e-commerce sites lead to similarly intermingled communications.[32] In such circumstances, there is a high risk that one user's right to be forgotten will unduly hamper others' free expression rights and leave intermediaries with the difficult, potentially impossible, task of "disentangling" individuals' data.

CDT cautions that a "right to be forgotten" will face significant international jurisdictional challenges and might hamper innovation and adoption of new services in the European Union. The dignitary interests found in European law are not reflected in all legal regimes worldwide. Accordingly, European citizens will likely not enjoy the same privileges while using foreign applications and services. Furthermore, services may be discouraged from serving the European Union directly or locating their businesses in EU member countries given the uncertainty and potential complications surrounding a "right to be forgotten." The Commission should take these serious challenges into account.

CDT also urges that any "right to be forgotten" not be interpreted so broadly as to give a data subject the right to compel a website (or other host) to remove information about her that she did not actively or passively create. Even setting aside the difficulties in authenticating the identity of the author of such requests, intermediaries and hosts should not be required or encouraged to act upon all requests from private parties to take down content created by another party.[33] Such a "right" would unfairly chill free expression and the free flow of ideas and information across the Internet. We would strongly reject a framework that imposes a duty to monitor posted content on the grounds of enforcing a "right to forget." (See *infra* for a discussion

[32] The "right to be forgotten" runs into tension with other projects, such as the U.S. Library of Congress's decision to archive every public "tweet" since Twitter's inception in March of 2006. *See* Matt Raymond, How Tweet It Is!: Library Acquires Entire Twitter Archive, Library of Congress Blog. April 14, 2010, *available at* http://blogs.loc.gov/loc/2010/04/how-tweet-it-is-library-acquires-entire-twitter-archive/.

[33] *See* Center for Democracy & Technology, *Campaign Takedown Troubles: How Meritless Copyright Claims Threaten Online Political Speech* (Oct. 2010) *available at* http://www.cdt.org/policy/cdt-releases-report-meritless-dmca-takedowns-political-ads.

of the question of intermediary liability and the Data Protection Directive.). Instead, a person demanding takedown of content she did not create should be required to obtain a judicial or administrative determination that the content in question is illegal and should be removed.

The Right to Data Portability Must be Carefully Defined

The Commission has requested comment on whether the principles of the Directive would be strengthened by the addition of a right to "data portability." CDT supports data subjects' ability to withdraw or obtain a copy of their own personal data from applications or services whenever feasible and when doing so does not infringe on the privacy rights of others. For example, individuals should have the ability to copy or move their blog posts, photos, and personal information on social networks. Data portability is not only an important element of user control but it also promotes innovation; services that make it difficult or impossible to export data can retain users without innovating because the cost of leaving will be too high for many users. CDT has thus encouraged online services to provide mechanisms for easily accessing and withdrawing personal information in a commonly accessible format.

Data portability, while desirable, is not always a straightforward process. CDT cautions that it can be difficult to ascertain when data is truly "one's own data." This is especially true in the social network context. For example, it remains an open question whether a list of an individual's friends "belongs" to that individual. Would the friends consent to their information being used with another service? Similarly, the nature of pictures, comments, or other materials that are shared among users of a social network is another gray area. Is this data "owned" by the poster or recipient? Taking these complexities into account, CDT recommends that any regulatory framework dealing with data portability contain a narrow definition of covered data so as not to inadvertently tread upon the privacy or free expression rights of others.

Finally, the Commission should ensure it is neither assuming the existence of technology standards that do not exist nor mandating the adoption of standards and hampering innovation. In sum, the Commission should avoid mandating a particular format in order to promote portability.

Creating Special Privacy Protections for Children May Impede Access to Information and Harm Privacy for all Users

With regards to transparency, the Commission seeks comment on introducing specific obligations for data controllers on the type of information to be provided to children and the modalities for providing it when describing online data collection and use practices. In all cases, CDT recommends providing clear, concise notice of data processing that is tailored to the data controller's audience. Thus, if a site or online service is specifically targeted to children,[34] it

[34] In the United States, the Federal Trade Commission determines whether a site or online service is targeted or "directed to children" (defined as minors under the age of thirteen) under its enforcement of the Children's Online Privacy Protection Act. Title 16 Code of Federal Regulations Section 312. The FTC considers a number of factors in making this determination, including "whether [a site's] subject matter and language are child-oriented, whether it uses animated characters, or whether advertising appearing on the website is directed to children." COPPA FAQs, "5. COPPA applies to websites or online services that are 'directed to children.' What determines whether or not a website or online service is directed to children?" *available at* http://www.ftc.gov/privacy/coppafaqs.shtm.

should provide notice of its data collection procedures in language and a format that can be understood by the children in its likely audience.

While the Commission is appropriately focused on providing increased transparency for child data subjects, CDT cautions the Commission that proposals to provide enhanced privacy protections for children who use the Internet could unintentionally infringe on children's rights to privacy or could inhibit older children's exercise, or adults' exercise, of rights to free expression (including the right to receive information). U.S. policymakers have recently considered these issues in connection with a consultation on the Children's Online Privacy Protection Act (COPPA), in which CDT filed extensive comments, and in connection with the work of a Congressionally-chartered Internet Safety Technical Task Force.[35]

In the U.S. proceedings, CDT and others noted that requirements to treat children differently from adults might be impossible to implement without collecting more data on children and adults alike, reducing privacy for all.[36] Information about the age of a data subject is not transmitted during the course of a typical Internet transaction, giving data controllers no way to segregate their data subjects by age with any degree of surety. Requiring collectors to discriminate among individuals by age could force data controllers to collect information on age or date of birth from *every* user in order to distinguish adult users from children.

Moreover, as CDT and others stressed to the FTC, this increased collection of information would likely chill users' expressive activity online.[37] Requiring users, including adults and older minors, to disclose personal information in order to access material online is a significant burden on the rights of free speech and access to information. Many individuals would likely be deterred from accessing legal content of a sensitive, personal, or controversial nature because they would be unwilling to provide personal information and compromise their anonymity in order to gain access to such material.

In addition, an obligation to collect age information from every data subject would place a burden on the expressive activities of website operators and other data collectors. Age verification procedures are expensive to implement, and this additional cost will hinder small innovators that attempt to launch new sites and services. Moreover, as the 2008 task force on Internet safety found, age verification technologies can be circumvented relatively easily, leaving website operators with no certainty that they could comply with a law requiring them to treat children's data differently.[38]

---

[35] COPPA is codified in Title 15, United States Code, Sections 6501-6506. Information about COPPA can be found at the FTC website, http://www.ftc.gov/privacy/privacyinitiatives/childrens.html and http://www.ftc.gov/privacy/coppafaqs.shtm. CDT's extensive comments on COPPA are available at http://www.cdt.org/blogs/emma-llanso/fine-coppa-indeed.

[36] Comments of Center for Democracy & Technology, the Progress & Freedom Foundation, and Electronic Frontier Foundation, in the Matter of Implementation of the Children's Online Privacy Protection Rule (Docket No. 339) ("Joint COPPA Rule Comments") 2, 7-9 (2010), *available at* http://cdt.org/files/pdfs/CDT-PFF-EFF_Joint_Comments.pdf; Supplemental Comments of the Center for Democracy & Technology, in the Matter of Implementation of the Children's Online Privacy Protection Rule (Docket No. 339) ("Supplemental COPPA Rule Comments") 3-5 (2010), *available at* http://www.cdt.org/files/pdfs/CDT_Supplemental_Comments.pdf.

[37] Joint COPPA Rule Comments 8-10, *available at* http://cdt.org/files/pdfs/CDT-PFF-EFF_Joint_Comments.pdf; Supplemental COPPA Rule Comments 3-5, available at http://www.cdt.org/files/pdfs/CDT_Supplemental_Comments.pdf.

[38] *See* Internet Safety Technical Task Force, Enhancing Child Safety & Online Technologies: Final Report of the Internet Safety Technical Task Force to the Multi-State Working Group on Social Netwoking of State Attorneys General of the United States 28-31 (2008),

The Commission must also carefully consider any approach that involves parents in protecting children's privacy. While it may be appropriate, even necessary, for a parent to have access to the data collected about a young child in order to review, correct, or delete it, and for a parent's permission to be required before a data collector can acquire a young child's data, older children have privacy rights in their own data and have a right to use the Internet to access information about sensitive topics including health, religion, and politics without seeking parental permission or having the information they may choose to store with such sites subject to parental review.

Protections for Intermediary Liability Are an Essential Element of Any Privacy Regime

Technological intermediaries such as ISPs, web hosts, and platforms for user generated content play an indispensible role in facilitating the free flow of information and stimulating online commerce. Any data protection regime must recognize the unique function of these entities in promoting freedom of expression, innovation, and economic growth in today's information-driven economies. While service providers should be held responsible for their own collection and use of personal data, these intermediaries should not be liable or responsible for the privacy infringing activities of their users.

As discussed above, online communication poses two kinds of privacy concerns: those stemming from a service's own collection and use of personal data, and those stemming from content authored or disseminated by third party users through sites for user generated content (UGC), such as social networks and video-hosting services. The first category of privacy concern is the key focus of the Directive.

CDT strongly believes that the liability of intermediaries for the second category of privacy concern—that is, privacy harms caused by third party content – should be limited. The creators of the content should remain liable, of course.[39] However, imposing on intermediaries liability for privacy violations committed by third parties would have a deleterious effect on the free flow of information and innovation online.[40] And the threat of intermediary liability could negatively impact user privacy and prevent effective implementation of the data minimization principle if service providers felt compelled to monitor their services or collect and retain more user data.

Europe has already confronted and seemingly resolved the issue of intermediary liability in the E-Commerce Directive, 2000/31/EC, which provides Internet intermediaries with significant protection from liability for content posted or transmitted by others and makes it clear that intermediaries are not responsible for monitoring their services.[41] When the E-Commerce Directive (ECD) was adopted, EU policymakers considered these protections indispensable for protecting the free flow of information and encouraging ICT development. U.S. law affords similar (and more robust) protections for intermediaries. The remarkable growth of the Internet

---

http://cyber.law.harvard.edu/sites/cyber.law.edu/files/ISTTF_Final_Report.pdf.

[39] While individual users should not be subject to all of the administrative provisions of the DPD, they should be liable for conduct infringing on the privacy of others under traditional principles.

[40] For more on the issue of intermediary liability in addressing unlawful behavior online, see Center for Democracy & Technology, "Intermediary Liability: Protecting Internet Platforms for Expression and Innovation" (April 2010), *available at* http://www.cdt.org/files/pdfs/CDT-Intermediary%20Liability_(2010).pdf.

[41] E-Commerce Directive, 2000/31/EC, Articles 12–14. The Directive also provides that states cannot impose on intermediaries a general obligation to monitor content hosted or transmitted on their services, nor a general obligation to actively investigate possible unlawful activity. Art. 15, E-Commerce Directive, 2000/31/EC.

and online services on both sides of the Atlantic has ratified the wisdom of those policy decisions.

Ten years later, however, the rules on intermediary liability have been opened to doubt in regards to privacy violations. Both the DPD and the ECD were written before the advent of Web 2.0 services, which provide platforms for UGC on a massive scale. These kinds of services support freedom of expression and access to information online in unprecedented ways, but were not contemplated by the DPD or the ECD.[42] As a result, the interaction between the ECD and DPD in the Web 2.0 environment has created some interpretations that are not optimal for privacy, free expression or innovation.

In particular, confusion has been created by an "exception" in the ECD that refers to the DPD: Article 1.5 of the ECD states that the ECD does not apply to "questions relating to information society services covered by" the DPD. The ECD also states in a cryptic recital that "application of [the ECD] should be made in full compliance with the principles relating to the protection of personal data, in particular as regards … the liability of intermediaries…"[43] The exception may just mean that intermediaries are subject to the DPD insofar as they collect information on their users. And the recital may mean that hosts, when notified of content that violates privacy, must take it down, just as they must take down any other illegal content upon notification. However, the "exception" language has been interpreted by some as meaning that the protections against intermediary liability in the ECD do not apply to privacy violations that are the fault of individual users of Web 2.0 services.

The Commission should clarify that Web 2.0 hosts and other intermediaries are not liable for content created by their users. Otherwise, the DPD could become a major impediment to the development of Web 2.0 services in Europe, for Web 2.0 hosts would be faced with the impossible task of ensuring that no content posted by any individual infringed on the privacy of anyone else.[44] The chill on free expression of such an approach would be significant. For many online services, the sheer volume of hosted UGC makes it impossible or economically unviable for a hosting platform to screen all content; imposing such liability on intermediaries would curtail the offering of such services in the EU.[45]

The issue can be resolved through application of the DPD's core concepts of "data controller" and "data processor." Most of the obligations of the Directive fall on controllers. The Commission should work with the Article 29 Working Party to make it clear that, in the Web 2.0 context, the data controller should be the person who posted the content to the UGC hosting service, while the provider of the platform itself should be considered to be only a processor with regard to that data. Defining Web 2.0 hosts as processors, not controllers, of UGC would reconcile the DPD and the ECD in a way that preserved the limitations on liability for

---

[42] User-generated content platforms often allow individuals with little technical knowledge or money to create, reproduce, disseminate, and respond to content in a variety of formats and with a worldwide audience.

[43] E-Commerce Directive, 2000/31/EC, Recital 14.

[44] To illustrate, the vast majority of routine conversation and reporting on social network sites – which very often mention people other than the author – could potentially violate someone's privacy, and the service provider would have no way of answering that question.

[45] For example, users post over 24 hours of video to YouTube every minute and an average of 750 tweets are posted to Twitter every second. Twitter Blog, *Big Goals, Big Game, Big Records*, June 18, 2010 *available at* http://blog.twitter.com/2010/06/big-goals-big-game-big-records.html; Caroline McCarthy, *New Year's Day breaks Facebook photo upload record*, CNET NEWS, January 4, 2011 *available at* http://news.cnet.com/8301-13577_3-20027212-36.html.

intermediaries.[46] This approach would leave online intermediaries responsible for safeguarding the personal data they collects about their users.

And it need not mean that there is no recourse for individuals harmed by third party users of an online service. Intermediaries can facilitate private or law enforcement action against wrongdoers – even anonymous and pseudonymous users – in response to a legitimate court order, under procedures that safeguard privacy and the threshold right of anonymity. CDT recommends that the Commission work with industry to document best practices among online service providers for safeguarding user and third party privacy where harmful content is posted by a user.

For further information, contact:

Justin Brookman
Director, Consumer Privacy Project
202-637-9800
justin@cdt.org

Cynthia Wong
Director, Global Internet Freedom Project
202-637-9800
Cynthia@cdt.org

Erica Newland
Policy Analyst
202-637-9800
Erica@cdt.org

[46] The Article 29 Working Party has issued two opinions that confused rather than clarified the relationship between the DPD and the intermediary liability provisions of the ECD. Article 29 Working Party, *Opinion 1/2010 on the concepts of "controller" and "processor"*, 00264/10/EN WP 169, p. 29 (Feb. 2010), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf, and Article 29 Data Protection Working Party, *Opinion 5/2009 on online social networking*, 01189/09/EN (June 2009). The Working Party opinion on social networking services (SNSs) concluded, with little analysis, that such services should be considered data controllers. The Working Party, however, did not draw any distinction between whether the social networking service is the controller of data it collects about its users – it clearly is – as opposed to whether the service is the controller of the data about others that is posted by a user. The Commission and the Article 29 Working Party should work to resolve this issue in a way that protects social networking services and other intermediaries from liability for the conduct of their users.