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

CDT ANALYSIS OF THE PROPOSED DATA PROTECTION REGULATION

March 28, 2012

I. Overview of CDT Analysis of the Proposed Data Protection Regulation

CDT welcomes the current review of the Data Protection Regulation as an important opportunity to advance policies that will enable data subjects to benefit from clearer, stronger privacy rules whilst allowing businesses to benefit from the single market and more consistent compliance mechanisms. Our comments are therefore aimed at achieving these two objectives. We note that this analysis does not address the parallel Directive legislation governing law enforcement access to personal data. CDT will release its analysis of that legislation at a later time.

Key Messages

- **CDT strongly supports** the use of the **Regulation instrument** to harmonize data protection across the common market and the renewed emphasis on **stronger enforcement** to provide data subjects with consistent, predictable privacy rights.
- **CDT proposes a clarification** that the Regulation's requirement of **parental consent** only applies when a controller has *actual knowledge* that it is processing a child's data, as opposed to *a presumption of knowledge* that it is likely processing data concerning a child. Otherwise, all controllers would have to adopt invasive, expensive, and ineffective controls to determine the identity of all data subjects in violation of Article 10 of the Regulation.
- **CDT urges significant revision** to the Articles providing for a **right to be forgotten** and for stringent rules around **profiling**, as these Articles are unduly broad and unworkable in their current iterations.
- **CDT supports a streamlined process** for the development of industry-specific **Codes of Conduct** and urges the Commission to take an active role in convening stakeholders around evolving privacy norms.

II. Expanded Analysis

Fundamentally, CDT supports the use of a Regulation to provide consistent privacy protections across the European Union. Varying country-level transpositions of the Data Protection Directive 95/46 (and more recently, the e-Privacy Directive 2002/58) have resulted in significant uncertainty for data subjects and companies, and have prevented the fundamental aims of this instruments from being fully realized. A Regulation that establishes a strong baseline for European data protection will be the most effective vehicle to assure

all EU citizens of meaningful data protection. We believe that member-state autonomy rights will be preserved by allowing derogations for additional levels of data protection consistent with country statutory and constitutional law, as well as expanded DPA authority to bring enforcement actions on behalf of data subjects.

Below, we provide comments on specific elements of the proposed legislation:

A. Expanded Definition of Personal Data

CDT supports the clarification that the definition of personal information includes "any information relating to a data subject." (Article 4(2)). Controllers increasingly are collecting and retaining information about data subjects in ways that are not always tied to real names, but that nonetheless threaten privacy rights. We are concerned, however, that the language contained in Recital 24 is potentially overly limiting. That Recital implies that online identifiers may be deemed personal information *only when* they may be combined with other information to "create profiles of the individuals and identify them." We have consistently argued that the focus on personally identifiable information (or information tied to a real name identity) increasingly makes little sense in the modern world, as data subjects have privacy interests in pseudonymous profiles not readily tied to a real name identity, and identifiability is an increasingly moving target that is difficult to frame in a binary fashion.[1] So long as the underlying substantive rules for the processing of personal data are reasonable and predictable, we believe that the Regulation should be applied to a flexibly broad conception of personal data that includes all facets of a data subject's identity.[2] (We are heartened to see that biometric information is rightfully included as an example of information that is quite clearly personal.)

However, data that is used or retained in a less identifiable format should not require protections that are as rigorous as those accorded data that is retained or used in a more identifiable format. While we recognize that nearly all personal data could hypothetically be tied back to an individual identity, data can be retained in a form that makes subsequent identification or reidentification considerably less likely. Such data would still be subject to the law and require substantive protections, but placing less onerous requirements on controllers could provide worthwhile incentives to controllers to keep data in a more obscure form. Similarly, we agree with the language in Recital 23 that data that has been rendered anonymous and not reasonably linkable back to an individual identity or device should not be subject to the Regulation's provisions. We suggest that the Regulation adopt a formulation for deidentification similar to that contained in the recent privacy report from the Federal Trade Commission: data is only deidentified (and thus outside the scope of the Regulation) when (1) the controller has taken steps to render the data reasonably unidentifiable, (2) the controller publicly commits not to attempt to reidentify the data, and (3)

[1] Center for Democracy & Technology, "Comments of the Center for Democracy & Technology Before the Federal Trade Commission in the Matter of Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Business and Policymakers," Feb. 2011,https://www.cdt.org/files/pdfs/20110218_ftc_comments.pdf.

[2] *Accord* Article 29 Data Protection Working Party, Opinion 01/201 on the data protection reform proposals (March 23, 2010) at 9-10, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf.

any third-party processors of the data are contractually prohibited from reidentifying the data.[3]

We strongly support the language in Article 10 making clear that controllers have no obligation to collect more data about a subject in order to comply with the terms of the Regulation. Requiring controllers to collect additional personal information in order to determine how to safeguard a data subject's privacy would obviously be a perverse outcome.

B. Lawful Basis for Processing and the Spectrum of Consent

CDT supports the Regulation's framework for consent. Under this framework, different categories of processing require different levels of consent from the data subject, ranging from explicit opt-in consent, to a right to object (opt out), to no consent needed whatsoever. (Articles 6, 19). However, the legislative language in Article 6 describing those categories of processing is vague, and may not offer predictability or certainty for either companies or individuals. While we recognize the need for flexibility under the new Regulation, we urge that these categories be more precisely defined.

Much of the initial criticism about the proposed Regulation has focused on the clarification in Article 4(8) that consent as a lawful basis for processing must be "freely given specific, informed, and explicit." Some commentators fear that as a result of this revised definition, controllers would have to bombard data subjects with unwanted requests for permissions for expected and uncontroversial data processing.

However, it is important to note that the Regulation allows alternative bases for lawful processing that are not based on consent. Some of these bases (Article 6(1)(b)-(c)) provide data subjects with no choice whatsoever, such as where the processing is necessary to perform a contract with the data subject. For other bases of processing, data subjects are explicitly given a "right to object" to the processing, which seems to correspond to the notion of "opt-out consent" in the United States. The primary difference, thus, between the US formulation and the model in the proposed Regulation is not structural. While recognizing categories of processing for which an opt-out is appropriate, the legislation is clear that by failing to take advantage of an "opt out" opportunity, the user has not meaningfully "consented" to the processing. Logically, we are sympathetic to this position, as merely having the ability to say "no" certainly does not mean in most circumstances that the users has consciously agreed to the processing. We also agree with the Commission that there should be lawful processing scenarios where a data subject should have the right to exercise an affirmative veto power that would render that processing unlawful.

However, while in theory we strongly support a spectrum of consent or user choice for data processing activities, we are concerned that the stated bases in the Articles may be too vague to offer certainty and guidance for data subjects and controllers. Particularly, Article 6(1)(f) which allows for processing when the controller judges that its legitimate interests outweigh the privacy rights of the data subject, and Article 19 which allows the controller to reject a data subject's opt-out for similar reasons, are vague, opening the door to

[3] This is the standard that has been proposed by the US Federal Trade Commission. *See* Federal Trade Commission (Bureau of Consumer Protection), Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers (March 26, 2012), available at http://www.ftc.gov/opa/2012/03/privacyframework.shtm.

interpretations that are either too expansive or too restrictive. We believe that this provision in particular must be clarified through a delegated act or one or more Codes of Conduct (under Articles 39 and 40).

Finally, we are concerned about the implications of Article 7(4), which states that consent may not be given if there is an imbalance of power between the controller and the data subject. One could make a convincing argument that there will *always* be "a significant imbalance between the position of the data subject and the controller" when the controller drafts the terms and conditions of a contract. Though we do not believe this is the intent of this provision, removing consent as a basis for lawful processing by companies who necessarily dictate the terms of a contract would force companies to find other bases for processing that give users less choice. Perhaps instead this provision could be revised by invalidating consent for unconscionable or unreasonable terms and conditions in contracts.

C. Profiling

We have significant concerns about the current iteration of Article 20 on "Measures based on profiling." Although we agree with the general principle that controllers should not amass opaque user profiles for potentially harmful purposes, the vague language in Article 20 is overly expansive and provides little certainty to companies about what sorts of activities are prohibited. CDT has been critical of the limited scope of the Fair Credit Reporting Act in the United States and the reluctance of the Federal Trade Commission to aggressively enforce its provisions; however, we caution that this Article arguably extends too far in the other direction and needs to be more precisely defined. As the language currently stands, controllers cannot reasonably be expected to be able to calculate when profiling may be deemed to "significantly affect" a natural person. The recitals are even vaguer, stating that individuals should not be subject to a "measure" based on profiling (Recital 58) absent very narrow, specified criteria. While we recognize that the proposed Regulation's formulation is narrower than the description in the recent Council of Europe recommendation on profiling, we urge that given the extremely stringent requirements for companies that engage in profiling behaviors, the language be tightened further to address only the specific class of profiling risks that warrant such limitations, and the Recitals should be amended to include illustrative examples of the specific processing behaviors sought to be covered by this Article, such as employment, credit, and insurance, and differential pricing.

D. Teens and Children

CDT supports the Regulation's treatment of teens' and children's data, though we urge that Article 8 be clarified to explicitly state that parental consent is only required when a controller has actual knowledge that a data subject is a child. The Commission notes several times that "children deserve special protection" in the context of data processing and defines "child" according to the UN Convention on the Rights of the Child, which is generally a person under the age of 18. We are pleased to see that Article 8, requiring parental consent for the processing of personal data of a child, is narrower in scope and applies only to the personal data of children under age 13. CDT has consistently advocated for older minors' free expression rights to access information, especially about potentially sensitive topics including health, religion, and political matters, without first obtaining parental consent. Indeed, the UN Convention on rights of the child itself recognizes that "child[ren] shall have the right to freedom of expression," and further

recognizes "the rights of the child to freedom of association and to freedom of peaceful assembly," and the obligations of parties to "ensure that the child has access to information and material from a diversity of national and international sources, especially those aimed at the promotion of his or her social, spiritual and moral well-being and physical and mental health."[4]

Within Article 8, we read "offering of information society services directly to a child" to mean that Article 8's obligations apply to data controllers with actual knowledge that a particular user is a child. We think that this is the right standard. Actual knowledge is a more workable, and privacy-protective, standard for age-based regulations than the alternative: requiring controllers to comply when they are presumed to have knowledge that some of their users might be children would require general-interest websites to collect more information from all users in order to distinguish children under 13 from adults and other minors. Such a requirement would bring Article 8 into conflict with proposed Article 10, which provides that data controllers "shall not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation." The Commission should clarify that Article 8 applies to controllers only when those controllers have actual knowledge that a user is under 13.

The current wording of Article 8 is, however, somewhat unclear; it could be read to mean that the Commission intends the verified parental consent requirement to apply to controllers who offer services targeted to children as a general matter — for example, websites dedicated to popular children's cartoon characters, or social networks aiming to serve pre-teen children. It would be reasonable to apply a verified parental consent requirement to those services clearly designed with young children in mind (as is the case in the United States),[5] but if this is the Commission's intent, it should state this plainly. We are concerned that attempts to read the current proposed language to cover these types of sites would result in the equivalent of a constructive knowledge standard. Such a standard would require that all general purpose websites obtain and authenticate the age of all users, in order to determine which ones are children deserving of heightened protection. This process would violate data subjects' privacy and their right to anonymity, impose massive compliance costs on companies, and ultimately be ineffective, as underage users could simply provide their parents' (or other adults') credentials. We urge that the text of Article 8 be clarified to ensure that a controller must obtain parental consent only when it has actual knowledge that a data subject is a child.

E. Right to be Forgotten

CDT recommends that Article 17 be narrowed to afford data subjects deletion rights for data they store with a controller. While CDT understands the privacy and dignity issues motivating proposals for a "right to be forgotten," we continue to have substantial concerns about both the proposal's effects on free expression and the technical difficulty of implementing such a regulation. For example, Article 17(2) would require that a controller take "reasonable steps, including technical measures" to inform third parties when a data subject has requested the erasure of previously public data, but this could prove impossible

[4] Article 13, Article 15 and Article 17, Office of the United Nations High Commissioner for Human Rights, Convention on the Rights of the Child (1990), *http://www2.ohchr.org/english/law/crc.htm*.

[5] *See* the Children's Online Privacy Protection Act, 15 **U.S.C.** §§ 6501-6508.

to implement. To identify these third parties, controllers would need to proactively search for the user's re-posted data or devise some way to keep track of which third parties had acquired the data when it was posted publicly, either of which would place an incredible burden on controllers, threatening the viability of user-generated content platforms. And, in either case, we believe there may be no reasonable steps that a controller could take to effectively limit the dissemination of previously public information by third parties. Placing notification requirements on such controllers could potentially be extremely burdensome with no concomitant value to data subjects, as whatever new controllers receive such notification would be under no obligation to obey deletion instructions.[6] Third-party controllers receiving these notifications would face the task of weighing the conflicting privacy and free expression interests of the data subject and the user who reposted the data, a task well outside these controllers' competency.

For example, presume that a politician makes a controversial statement on his Facebook page. To the extent that Facebook is a platform for the politician's own speech, it is reasonable to allow that politician to delete the post from Facebook if he later regrets the statement. However, if a blogger reports on the post on Wordpress.com, or a data subject places a screenshot of the offending post on his Twitter account, it would violate the free expression rights of those individuals to require them to delete their own posts, or to force Wordpress or Twitter to remove their users' content because they truthfully report the personal information of another data subject.[7]

Instead of a vague and impractical "right to be forgotten" that cannot be meaningfully delivered to data subjects, CDT strongly supports the right to erasure of data provided to a controller to store or host, which is a narrower formulation than the language in the proposed Regulation. We believe that the language contained in Section Three of the recent settlement agreement between the Federal Trade Commission and Facebook is a reasonable middle-ground approach on the erasure issue, one which appropriately balances the interests of privacy rights, free expression rights, and practical compliance for data controllers and processors.[8]

---

[6] Such third-party notification provisions could be appropriate if they are limited to data processors with which the controller had purposefully stored the individual's data.

[7] CDT's views are closely aligned with the European Data Protection Supervisor on this issue http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf ("The EDPS welcomes this provision, but emphasizes that the right to be forgotten must be effective in reality. It may in some cases be a huge effort to inform third parties who ma be processing such data, as there will not always be an understanding of where the data may have been disseminated. To have an effective right to be forgotten implies that the scope of the right should be clear from the moment the Regulation applies. Article 17 might need to be further developed in that respect.").

[8] "It is further ordered that Respondent and its representatives, in connection with any product or service, in or affecting commerce, shall… implement procedures reasonably designed to ensure that covered information cannot be accessed by any third party from servers under Respondent's control after a reasonable period of time, not to exceed thirty (30) days, from the time that the user has deleted such information or deleted or terminated his or her account, except as required by law or where necessary to protect the Facebook website or its users from fraud or illegal activity. Nothing in this paragraph shall be construed to require Respondent to restrict access to any copy of a user's covered information that has been posted to Respondent's websites or services by a user other than the user who deleted such information or deleted or terminated such account." *In the Matter of Facebook, Inc., a corporation, Agreement Containing Consent Order,* FTC File No. 092 3184, http://ftc.gov/os/caselist/0923184/111129facebookagree.pdf.

Finally, Article 17(1) seems to conflate the right to be forgotten with other issues such as data minimization and lawfulness of processing. Article 17(1)(a) and (d) state that a data subject shall have the right to request deletion of data when the data is no longer necessary for a legitimate purpose or when the processing does not comply with the Regulation, respectively. A controller is already prohibited from collecting or retaining data under those scenarios; granting data subjects a right to remind controllers of their legal obligations seems superfluous.

F. Data Portability

CDT supports the inclusion of a right to data portability in the proposed Regulation, as we believe that an expectation of data portability is fundamentally necessary if users are to adopt and trust cloud computing platforms. (Article 18) However, we are not convinced that it is appropriate to delegate to the Commission the authority to dictate the specific technical formats and procedures that controllers must follow in making data available to their users. Such formalized rules could stifle the innovation of superior formats and processes and could also subject controllers to disparate rules in other jurisdictions. Rather, we recommend that Article 18 require that data be made available in a commonly used format and that the procedures must be sufficiently simple and usable such that users can readily take advantage of them. Robust regulatory enforcement against companies that put unreasonable barriers to data portability is a better control on making formats usable than is a Commission rulemaking that could fail to keep up with emerging technologies and could conflict with requirements in other jurisdictions.

G. Privacy by Default

We advise against any mandate that data subject information must not be shared publicly by default. (Article 23(2)). There are many services that are specifically designed as platforms for public communication, such as web hosting services like Tumblr and Twitter. While those services should offer robust tools to shield certain (or all) information from the eyes of the general public, there is no reason those controls should be turned on by default if they are contrary to the fundamental nature of the services and to how most users would wish to use them. Moreover, a default requirement may have the perverse effect of discouraging controllers from developing and offering more sophisticated and targeted privacy tools. The promotion of other measures – such as clear and conspicuous disclosure of privacy choices, a privacy prompt forcing users to make privacy decisions (a forced choice rather than a default),[9] periodic notice and reminder about existing privacy settings and available controls –would represent a more reasonable approach to preserve user privacy,

H. Security and Data Breach Notification

CDT supports Article 30's requirement that companies deploy reasonable security measures while balancing the sensitivity of the protected information, evolving technology, and implementation costs. However, we do not believe it is appropriate to grant the Commission the authority to specify particular technological solutions or measures to safeguard personal data. It is extremely unlikely that the Commission could sufficiently

[9] *See* Justin Brookman, "Closing Pandora's Box," Center for Democracy & Technology Policy Beta Blog (Aug. 4, 2010), https://www.cdt.org/blogs/justin-brookman/closing-pandora%E2%80%99s-box.

update these requirements in real time going forward, and granting the Commission this authority would disincetivize security innovation, freezing data protection at a static floor that would be well-known by malevolent actors. We believe it would be more appropriate to simply require "reasonable" security protections, with the parameters of what constitutes reasonable being worked out through enforcement on a case-by-case basis. (see also, *infra*, §N "Open Ended Commission Authority and Tech Mandates")

CDT has supported the development of privacy breach notification laws in the United States, and we are pleased to see that the new Data Protection Regulation will require notice to data subjects when their personal information has been compromised.[10] In addition to protecting data subjects' inherent privacy rights, this provision provides strong incentives to controllers to safeguard personal information, by exposing them to significant costs in the event of data loss (regardless of fault). We have typically argued against personal notification requirements that hinge upon an affirmative finding that a data subject is likely to be harmed; instead, we propose to switch the burden and recommend notification to a data subject whose information has been breached *unless* the controller determines there is likely to be no adverse impact. We do support a requirement that the lead DPA be notified regardless of such a finding, though we disagree with the requirement that a DPA must affirmatively approve a request not to notify individuals because the controller believes that the data was sufficiently encrypted or otherwise protected (Article 32(3)). We do not believe this latter scheme is scalable and administrable, and recommend instead that the DPA receive notice of such a determination, based on which it could object to the controller's conclusion and require individual notification.

Although the 24-hour DPA notification requirement has been softened since the inter-service review, we still believe that even guidance that reporting should happen within 24 hours is unreasonable, as in the vast majority of data breach scenarios, a controller or processor will not be able to say with a high degree of confidence even what data had been breached after just 24 hours. State breach notification laws in the United States have typically required notification to data subjects and regulatory authorities within 30 or 60 days, though we support the language found in many laws requiring notification "as soon as practicable" and "without undue delay." Even without a strict timeline, regulators will be able to bring enforcement actions against entities that delay unreasonably, as has been the case in the U.S.[11] Furthermore, while we are skeptical about the value of some of the mandatory documentation provisions in other sections of the proposed Regulation (see *infra* §I "Privacy by Design and Privacy Impact Assessments"), the documentation requirements around a data breach incident seem worthwhile and reasonable.

I. Privacy by Design and Privacy Impact Assessments

CDT urges that the Regulation focus on affording data subjects substantive privacy rights, and focus less on dictating the process controllers and processors must

[10] The scope of breach notification in the proposed Regulation is considerably broader than in any U.S. law, expanding beyond sensitive financial and health information to any "personal data." While there has been discussion in the United States about expanding data breach requirements to email addresses (to prevent phishing attacks after a breach), requiring potentially expensive notification for *all* data breach events (such as the loss of IP logs that would not be easily attributable to individuals) may be unduly burdensome without commensurate benefits to individuals.

[11] Sharon Gaudin, *New York AG Gets First Settlement under Security Breach Notification Law*, INFORMATIONWEEK, April 27, 2007, http://www.informationweek.com/news/199202218.

utilize to ensure those rights. We support the concept of "privacy by design," and we believe it is appropriate to require some level of internal process to ensure that privacy risks and threats are considered throughout a product's lifecycle. However, as noted above in our discussion of security, we believe that regulators' primary function is to develop substantive privacy rules for companies to follow, not internal business processes. In theory, if regulators sufficiently identify and punish bad privacy practices (by clarifying the scope of the law and increasing enforcement actions), companies will have strong incentives to develop programs to build privacy into products.

That said, in the US, we have seen that many companies have not fully appreciated the risk and costs associated with potential data breach scenarios, and many large, supposedly sophisticated companies have failed to implement even rudimentary (and often, inexpensive) security practices, sometimes leading to incredibly expensive notifications and enforcement actions. On the other hand, we have also seen law prescribe particular burdensome business processes that have fundamentally failed to protect individual privacy.[12] Thus, we believe that a reasonable middle-ground approach is to require that companies develop a process to assess and internalize risk without being overly prescriptive about how to do so. (See also, *infra*, Section N, "Open-Ended Commission Authority and Tech Mandates"). For that reason, we are unsure that mandating a dedicated Data Protection Officer will always be a cost-effective means for to ensure better data privacy practices.

We have also supported the idea of requiring "Privacy Impact Assessments" under certain circumstances,[13] but we are dubious about their value if they are to be made available to DPAs. As we have previously argued to the U.S. Department of Commerce on their suggestion that companies make PIAs publicly available, such PIAs would be drafted only for DPA or public consumption, and would not represent an honest, rigorous assessment of any potential privacy risks. We believe that a true privacy impact assessment can only be conducted if the audience for the assessment is internal decisionmakers. A PIA will only serve a useful purpose if it forces a company to consider the privacy impact of certain business operations, not if it is merely a defensive document designed to insulate a company from liability (as many privacy policies are today). For the same reason, we do not believe that PIAs should be provided to data subjects for commentary as provided in Article 33(4); such PIAs would cease to be a rigorous evaluation of privacy risks and would be written entirely for public consumption.

J. Lead Regulator

We support the appointment of a lead regulator in Article 51(1) for administrative purposes, though we believe the consistency mechanism should be clarified to ensure that other state DPAs can act to protect their citizens. To the extent that the proposed Regulation places affirmative, *ex ante* administrative burdens on companies, we fully support the idea that only one DPA should be setting the parameters for that compliance instead of twenty-seven. Similarly, we support the use of lead regulators in

[12]Federal Trade Commission et al, "Federal Regulators Issue Final Model Privacy Notice Form," (Nov. 2009), http://www.ftc.gov/opa/2009/11/glb.shtm.

[13] However, the categories of processing requiring PIAs (and prior authorization in Article 34) are in some instances too vague and should be clarified or narrowed, especially 33(2)(a) which mirrors the language on profiling in Article 20, (*see supra*, §C. Profiling) and 34(2) requiring consultation for "specific risks."

approving applications for the approval of Binding Corporate Rules, and would also support lead regulator (or alternatively European Data Protection Board) approval for Codes of Conduct, again instead of twenty-seven separate DPAs' approval. We also agree with those who argue that the all subsidiaries of a corporation should also be regulated by the same lead regulator, rather than different corporate structures under common control being subject to different lead DPA authority across the EU.[14]

However, we have concerns that the proposed Regulation may unduly limit state DPAs that are not lead regulators to bring *enforcement* actions against controllers that misuse personal data. We believe that so long as the substantive data protection rules are clear and predictable, member state DPAs must have a reasonable means to act to defend their citizens' rights.[15] The proposed regulation does suggest a framework for member state cooperation in enforcement actions, but the structure seems unduly cumbersome and bureaucratic, and it could well prevent DPAs from acting with sufficient speed in addressing violations of the Regulation. We are concerned that lead DPAs who suddenly gain primary responsibility for a wide range of companies could easily become overburdened, and they may lack the resources (or the will) to bring meaningful enforcement actions. While inconsistency across the EU has been a persistent problem with the current data protection framework, we believe that this has stemmed primarily from inconsistent substantive obligations (as different member states have transposed the Directive differently) and from *sporadic* enforcement, not contradictory enforcement. We believe that Articles 56-63 on the joint operations of supervisory authorities and the consistency mechanism should be clarified to ensure that all DPAs have the authority to meaningfully act on behalf of their citizens.

K. Increased Penalty Authority

CDT supports giving Data Protection Authorities greater authority to obtain meaningful penalties from controllers that violate individual privacy rights, but suggest the language be modified to ensure that penalties are reasonable, proportionate, and appropriate. (Articles 77, 79) CDT has long believed that one of the greatest weaknesses of the European data protection regime has been the lack of robust enforcement,[16] and we support the move to give state Data Protection Authorities stronger authority to obtain dissuasive administrative sanctions (Article 79). The criteria for assessing an appropriate sanction are by and large sound, however we believe they should be expanded to consider additional, potentially mitigating factors. In order for the administrative sanctions provision to be truly "proportional" as stated in the proposed legislation, we believe that the number of affected EU citizens and an evaluation of the

[14] Hogan Lovells International LLP, Response to the Ministry of Justice's Call for Evidence on the EU Data Protection Proposals (2012) at 2-3, http://www.hoganlovells.com/custom/blogs/hldataprotection/Hogan_Lovells_Submission.docx.

[15] *See also* European Data Protection Supervisor, Opinion of the European Data Protection Supervisor on the Data Protection Reform Package (March 7, 2012), at ¶ 237 (asserting "the view that the role of a lead authority should not be seen as an exclusive competence, but rather as a structured way of cooperation with other competent supervisory authorities, as the 'lead authority' will depend heavily on the input and support of other supervisory authorities at different points in the process"). http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf.

[16] Erica Newland, "CDT Comments on EU Data Privacy Directive," *Center for Democracy & Technology Policy Beta Blog* (January 2011),https://www.cdt.org/blogs/erica-newland/cdt-comments-eu-data-protection-directive.

impact that a sanction would have on a company's business should be among the factors considered by DPAs and courts in determining fair awards. We also believe that procedural violations of the Regulation (such as certain prescribed "privacy by design" considerations) should not necessarily in themselves be a basis for administrative sanction, but could be a factor for DPAs to consider in determining an appropriate award. Finally, we believe that administrative sanctions should be optional at the discretion of the DPA, not mandatory.

We also question the language in Article 77(2-3) that mandates joint and several liability for all controllers and processors absent an affirmative showing by each that they were not responsible. Mere contractual relationship between processors and controllers should not trump a DPA's obligation to demonstrate fault and liability for any particular actor. We do not believe that a requirement to make an affirmative case against each party will meaningfully hamstring DPAs' ability to enforce the regulation.

L. Free Expression and State Derogations

CDT believes that fundamental rights such as free expression should be addressed not through member state derogations, but should be provided for in the Regulation. (Article 80) We support the idea expressed in Article 80 that there should be exceptions to the data protection rules to protect the free expression rights of users and journalists, as recognized in, *e.g.*, Article 10 of the European Convention on Human Rights. We believe, however, that the Regulation should provide directly for the necessary exemptions for the protection of individuals' free expression rights rather than leave it to the member states to enact derogations. We are concerned that the lack of a uniform framework outlining the scope and practical design of such exceptions will lead to uncertainty, both among Member States attempting to balance free expression rights with the requirements of the Regulation and among data controllers themselves; this uncertainly would have a chilling effect on press organizations and user-generated content platforms. In addition to providing clear exceptions to accommodate the processing of personal information for journalistic purposes and artistic or political expression, the Regulation should continue to allow for additional derogations by member states that have or wish to adopt additional or broader protections for free expression.

M. Multistakeholder Development of Industry-Specific Rules

CDT supports a streamlined process for the development of industry-specific Codes of Conduct and urges the Commission to take an active role in convening stakeholders around evolving privacy norms. (Article 38) CDT was founded on the idea that a consensus-based approach to solving online problems can often adapt most quickly to changing technologies and individual perceptions about privacy and other fundamental rights. Over the years, we have intermediated discussions among industry and other civil society groups to put forward best practices guidance on a wide range of issues, such as the use of RFID technology,[17] financial data transfer among vendors,[18] mobile application

[17] *See* "CDT-Led Working Group Releases RFID 'Best Practices,'" Center for Democracy & Technology (May 23, 2006), https://www.cdt.org/policy/cdt-led-working-group-releases-rfid-best-practices.

[18] *See* Justin Brookman, "Best Practices: Online Subscription Upselling," Center for Democracy & Technology (February 28, 2012), https://www.cdt.org/blogs/justin-brookman/2802best-practices-online-subscription-upselling.

privacy,[19] and how to fight spyware.[20] We have long believed that Codes of Conduct, negotiated with both companies and representatives of civil society as participants in the discussion, will often be the most effective and flexible means of translating the high-level Fair Information Practice Principles into operational practices for specific, divergent industries.[21] We support the language in the proposed Regulation granting the Commission the authority to endorse specific Codes of Conduct that would be enforceable on an EU-wide basis.[22]

We would urge, however, that the Commission be given a greater responsibility in convening stakeholders to address privacy issues. In the U.S., we have supported the Obama administration's recent call for enforceable codes of conduct as part of a legislative solution in the United States. The White House proposal calls for the National Telecommunications and Information Administration (a division under the President's executive authority) to affirmatively convene industry, regulators, and civil society representatives to address emerging privacy issues that perhaps would not even have been envisioned when legislation was first enacted.[23] We believe that the European Commission should serve a similar role in bringing stakeholders together to monitor the evolving privacy landscape to ensure that the new Data Protection Regulation is sufficiently flexible to address new threats to individual privacy while avoiding rigid mandates that would chill innovation or become quickly outdated.

N. Open-Ended Commission Authority and Tech Mandates

CDT supports the use of delegated acts to develop precise data protection rules, but urges that the Commission not require specific technical mandates in implementing this Regulation. We believe that details of implementation of the Regulation across diverse industries should not be included within the text of the Regulation itself, as narrow, prescriptive language in the Regulation could lose relevance as technology evolves and could chill innovation. For that reason, where a multistakeholder approach fails to result in a Code of Conduct or other sufficient guidance, delegated acts by the Commission would be a preferable means to set privacy rules rather than more rigid legislation. When the Commission does determine that a delegated act is appropriate, we urge that the process or determining and issuing such an act is fully transparent and open to consultation with stakeholders, including industry and civil society.

We advise against several provisions within the proposed legislation that delegate to the Commission the authority to issue specific technological mandates for companies to adhere to. We believe that tech mandates are counterproductive, quickly become outdated, and

---

[19] *See* "Best Practices for Mobile Applications Developers," Center for Democracy & Technology (December 2011), https://www.cdt.org/blogs/2112best-practices-mobile-applications-developers.

[20] *See* Anti-Spyware Coalition, www.antispywarecoalition.org.

[21] See, e.g., Statement of Leslie Harris Before the House Committee on Energy and Commerce, The Best Practices Act of 2010 and Other Federal Privacy Legislation, July 22, 2010, http://www.cdt.org/files/pdfs/CDT_privacy_bill_testimony.pdf.

[22] *See also* Ira S. Rubinstein, Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes, 6 I/S, J. LAW AND POLICY FOR THE INFORMATION SOCIETY 356 (2011).

[23] *See* "CDT Comments on NTIA Multistakeholder Process to Develop Privacy Codes of Conduct," Center for Democracy & Technology (April 4, 2012), https://www.cdt.org/comments/cdt-comments-ntia-multistakeholder-process-develop-privacy-codes-conduct.

discourage new solutions. We would instead urge that delegated acts merely require substantive results, rather than specific technological processes to achieve those results.

0. Intersection with e-Commerce Directive

Finally, we believe that this Regulation would be most effective if it were amended to subsume the e-Privacy Directive as well as the Data Protection Directive. As noted in Recital 13, data protection regulation should be "technologically neutral"; as the boundaries between online and offline data collection and processing merge, it increasingly makes less sense to treat them pursuant to divergent legal regimes. We do, however, strongly support the language in Recital 17 stating that the Regulation should have no effect on the immunity provisions for intermediary service providers contained in Articles 12 and 15 of the e-Commerce Directive.

For further information, please contact

Justin Brookman
Director, Consumer Privacy
+1 202-637-9800
justin@cdt.org

Caroline De Cock
+32 (0)474 840515
cdc@n-square.eu