COMMENTS OF THE AMERICAN BAR ASSOCIATION SECTIONS OF ANTITRUST LAW AND INTERNATIONAL LAW ON THE PROPOSED REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE EUROPEAN COUNCIL ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA AND ON THE FREE MOVEMENT OF SUCH DATA

November 20, 2012

The views stated in these Comments are presented on behalf of the Section of Antitrust Law. They have not been approved by the House of Delegates or the Board of Governors of the American Bar Association and therefore may not be construed as representing the policy of the American Bar Association.

The Sections of Antitrust Law and International Law (the "Sections") of the American Bar Association respectfully submit these comments to the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) (the "Draft Regulation"). In its Communication to the European Council and Parliament on January 25, 2012 transmitting the Draft Regulation and explaining its timing and rationale, the Commission invited input from all interested parties so that a full, robust and informed dialogue can contribute to the final shape and implementation of the Regulation. These comments are intended to further this dialogue, and reflect the Sections' experience in international and cross-border privacy and data security issues. The Sections' long involvement in these issues rests on the participation of both private and public sector lawyers, economists and market participants, reflecting the interests of all those who engage in, benefit from, and enforce legal rights relating to digital as well as traditional commerce in which personal data plays an important role. The Sections do not advocate on behalf of any particular interest or party; rather, we offer our comments as constructive input of the type invited by the Commission.

The Sections commend the Council for presenting a comprehensive Regulation that takes into account the vast technological changes and legal developments that have occurred since the enactment of the 1995 Data Protection Directive and its implementation in the Member States' national laws. The Sections also commend the substantial improvements embodied in the current draft, particularly with regard to recognizing the need to foster international cooperation in cross-border law enforcement. The Sections believe that the harmonization reflected in the Draft Regulation's legal standards and enforcement provisions represents a substantial and positive development in EU privacy and data security law. In these Comments, we make several suggestions that we believe both further the goals of modernization and harmonization and serve the desired balance between individual privacy and the development of information markets and services that benefit EU nationals.

1. Executive Summary

These comments make the following points:

- The limits on extraterritorial application of EU privacy laws currently embodied in the Data Protection Directive and carried out in current practice should be maintained in the Draft Regulation.

- The Draft Regulation should recognize contextually-based consent in connection with the continued use and processing of information voluntarily provided by data subjects.

- The Draft Regulation should adopt community-wide standards applicable to cloud computing applications and services without resort to delegated acts mechanisms, and should expand the adoption of Binding Corporate Rules for cloud processors and the transfer of depersonalized data to servers located outside of the EEA where adequate security measures are taken to protect that data.

- The Draft Regulation should expressly acknowledge that conflicting legal obligations may in some instances justify exceptions to the Regulation's requirements to the extent necessary for data controllers and processors to discharge those obligations.

- The "right to be forgotten" should be implemented as a set of principles recognizing data subjects' ability to cause the deletion of their personal information from digital memory where appropriate rather than as an overriding personal right that may conflict with the need of some data controllers to maintain that data.

- The period for the initial reporting of data breaches to supervisory authorities should be lengthened from the proposed 24 hours to a period that better accommodates the time needed to adequately identify, investigate and diagnose the circumstances of the breach. In addition, the content and prescribed methods of notification should be governed by a community-wide standard and should not be subject to delegated acts mechanisms.

- The new and substantial fines authorized by the Draft Regulation should be reduced and phased in over time, should be discretionary rather than mandatory, and should be coordinated among the supervisory authorities such that a party will not be subject to duplicative punishment.

2. Extraterritorial Application of EU Law

The Draft Regulation by its own terms extends the territorial reach of EU privacy law in new ways. Specifically, it provides that the obligations of EU privacy law extend to entities

outside of the EU if those entities (1) offer goods or services to data subjects in the EU or (2) "monitor the behaviour" of those data subjects. The concept of "monitoring the behaviour" of data subjects is meant, according to the draft Regulation's recitals, to encompass online behavioral advertising or other activities commonly undertaken to compile information on data subjects.

This provision is a significant expansion of current EU data protection law. Under the existing EU Data Protection Directive, entities operating outside of the EU will be subject to the application of EU law only if they are either established within an EU Member State or they use equipment (particularly servers) located in the EU to collect information on EU data subjects.[1] Although EU enforcers have in some circumstances taken the position that extraterritorial application of EU privacy obligations may be triggered by non-EU sites' deployment of standard Internet technologies such as browser cookies and Javascript,[2] the extraterritorial application of EU privacy obligations has not previously been extended as far as would be the case under the Draft Regulation. The Draft Regulation thus represents a significant expansion of the applicability of EU law.

In the Sections' view, a more balanced and workable approach is that taken in the EU Directive on Privacy and Electronic Communications (the "E-Privacy Directive"). Article 3(1) of the E-Privacy Directive provides that it "shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks *in the Community*."[3] Accordingly, conduct regulated by the E-Privacy Directive is limited to communications provided by services on European public communications networks. The Czech Republic advocated a similar approach in its comments on the Draft Regulation.[4] We believe this approach should be continued in the new data protection framework.

The Sections believe that adopting the limitations contained in the E-Privacy Directive is a sound solution. These limitations, where consistently applied, have served to encourage the promulgation of domestic privacy and data protection regulations around the world.

3. Consent

The concept of informed consent of data subjects as a prerequisite to the gathering, processing, and disclosure of their personal information long has been a cornerstone of EU privacy law. The Draft Regulation substantially changes the definition of effective consent and its limitations in ways that we believe may have significant unintended consequences,

---

[1] *See* Data Protection Directive 95/46/EC, Art. 4(1).

[2] *See* Article 29 Working Party, Working Document on Determining the International Application of EU Data Protection Law to Personal Data Processing on the Internet by Non-EU Based Web Sites (April 2002) , *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp56_en.pdf.

[3] Directive (EC) 2002/58 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 [2002] OJ L201/37 (emphasis added).

[4] "It is doubtful to extend the jurisdiction of the EU outside of its territory. It is not clear which instruments the Member States should use to enforce duties stipulated by regulation on such broad scope. The Commission certainly did not offer any. Instead, Art. 4(1)(c) of the Directive should be reused." Note from General Secretariat to Working Group on Information Exchange and Data Protection, Council of the European Union, 2012/0011 (COD), 18 July 2012, at 13.

particularly where consent is the primary legal basis on which personal data is processed. While we recognize that these proposed developments are intended to give data subjects increased control of the collection and use of their personal data, mandating a particular form of consent actually may inhibit the efficient and appropriate use of personal information for the benefit of the data subject.

Under current EU data protection law "consent" is defined as "any freely given specific and informed indication" by which the data subject "signifies his agreement to personal data relating to him being processed."[5] The Draft Regulation would change this definition substantially by requiring that consent be "explicit." This heightened standard necessarily requires some expression above and beyond "unambiguous consent," the current principal basis for permitted data processing.[6] Furthermore, under the Draft Regulation, consent would only be considered sufficient where there is a statement by or a clear affirmative action of the data subject."[7] Arguably, then, many forms of implied or opt-out consent would be insufficient justification for processing personal data.

We believe that eliminating reliance on opt-out consent could negatively impact the online and mobile markets in critical ways. Most online advertising networks, both in Europe and globally, rely on expressions of implied or opt-out consent as a basis to process that user's personal data. In addition, online operators that provide goods and services use opt-out consent to process personal data once the initial, opt-in consent event has occurred. Opt-out consent preserves the fluidity of the user's online experience by avoiding an intrusive consent mechanism each time an advertisement is served or other interaction occurs. Rather, continued consent is implied, unless the user indicates otherwise. In addition, implied or opt-out consent does not require the user to take an affirmative action to signal consent, but rather recognizes that the user has consented to the practice. Requiring that a user affirmatively indicate his or her consent each time an interaction occurs may downgrade the user experience, a consequence that is recognized as a hindrance to the development of the digital ecosystem.

The Sections believe there is an alternative approach that will both preserve user control and choice while providing online operators the needed flexibility to preserve the online experience. This approach would be to adopt a "contextual" standard that defines the consent obligation based on the context and privacy expectations of the transaction. For example, consider the contextual standard to define a consent obligation for the collection of geo-location data through a map application on a smart or GPS-enabled phone or other device. While geo-location data is sensitive, requiring express or opt-in consent each time geo-location data is collected may disrupt the user experience. Instead, express or opt-in consent may be required the first time geo-location data is collected; implied consent becomes the basis for subsequent collections; and use is permitted because the user has expressly consented to this data gathering by affirmative agreement. This contextual solution is more in line with the user's privacy

[5] Directive 1995/46/EC, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:NOT

[6] Consent is one of the six bases by which personal data can be lawfully processed under European data protection law. The other five bases are: unambiguous consent, compliance with a legal obligation, to protect the vital interests of the data subject, in the public interest or in an official capacity, and legitimate interests pursued by the controller (except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject). Directive 95/46/EC, Section II, Article 7

[7] Recital 25

expectations and interaction with the map application, given that the application requires access to the user's geo-location data to continue to provide the requested service.

The contextual approach to consent already has been endorsed by other privacy enforcers and could serve as an important point of harmonization between EU and other data protection regimes.[8] We also note the use of a contextual standard in the guidance prescribed for compliance with the UK's Cookie Law. [9]

4. Cloud Computing

Cloud computing represents a substantial change in how information technology and digital services are performed and distributed, with the potential for dramatically increasing the efficiency and availability of electronic commerce. The Article 29 Working Party describes cloud computing as consisting "of a set of technologies and service models that focus on the Internet-based use and delivery of IT applications, processing capability, storage and memory space" and is offered through a wide range of services by cloud providers.[10] Indeed, the advent of cloud computing is recognized within the EU as creating the opportunity for substantial community-wide economic benefit.[11]

The Draft Regulation generally will facilitate the deployment of cloud computing. The Sections note two points of potential conflict that we believe should be considered and addressed. First, the Draft Regulation's reliance on the delegated acts and implementing provisions granted to the EC creates the possibility of inconsistent regulation that could adversely impact the beneficial deployment of cloud computing solutions. An important advantage of cloud computing is the efficiency created through the ability to use the Internet to move data to servers in various locations, which includes moving data throughout the EU. Harmonized standards are required to facilitate this intra-community transfer of data. Without

---

[8] See, e.g., FTC Report: Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers (March 2012) at p. 48**,** *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf ("For practices requiring choice, companies should offer the choice at a time and in a context in which the consumer is making a decision about his or her data.")**;** see also Consumer Data Privacy In A Networked World: A Framework For Protecting Privacy And Promoting Innovation In The Global Digital Economy at p. 9-10 , available at: www.whitehouse.gov/sites/default/files/privacy-final.pdf ("The Consumer Privacy Bill of Rights reflects the FIPPs in a way that emphasizes the importance of context in their application. Key elements of context include the goals or purposes that consumers can expect to achieve by using a company's products or services, the services that the companies actually provide, the personal data exchanges that are necessary to provide these services, and whether a company's customers include children and adolescents.).

[9] See Guidance on the Rules for Cookies and Similar Technologies, UK Information Commissioner's Office (May 2012) *available at* http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/the_guide/~/media/documents/library/Privacy_and_electronic/Practical_application/cookies_guidance_v3.ashx

[10] Art. 29 Data Protection Working Party, *Opinion 05-2012 on Cloud Computing*, 4, 01037/12/EN, WP 196, (July 1, 2012), available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf [hereinafter Art. 29 Working Party Cloud Computing Opinion].

[11] At the time the Draft Regulation was first announced, Neelie Kroes, Vice President of the EC responsible for the Digital Agenda, in a speech regarding EU data protection reform and cloud computing stated that cloud computing "will change the way businesses do IT" and that the appropriate regulatory inquiry should focus on "how to make Europe not just Cloud-friendly – but Cloud active." Ms. Kroes noted that "it's no use having rules that only make sense on paper, but are unworkable when it comes to new technology and can't be applied in practice." Neelie Kroes, *EU Data Protection Reform and Cloud Computing*, Speech Before the "Fueling the European Economy" Event (Jan. 1, 2012), SPEECH/12/40, available at http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/40.

revision to the authority and autonomy of the supervisory authorities, real harmonization is not fully possible. Each supervisory authority will have both enforcement and investigatory authority and the authority to determine what data processing requires prior approval. This division of authority has the potential to result in varying requirements and enforcement for the exact same cloud computing services provided across member states.

Another serious obstacle to the growth of cloud computing relates to the transfer of data in the cloud to servers located outside the EU. Such transfers are necessary to take full advantage of the benefits of cloud computing efficiencies and to avoid possible technical limitations created by infrastructure restrictions.[12] To the extent that the Draft Regulation would inhibit the exchange of data within the cloud, the benefits of this functionality may be lost or impaired.

We suggest that there are two ways to address the limitations created by the Regulation on transfers of data in the cloud to servers outside the EU. First, there is ongoing consideration of allowing data controllers and processors to participate in the Binding Corporate Rule process. We strongly recommend that this expansion of access to Binding Corporate Rules be included in the final Regulation. Other innovative approaches to facilitating data transfers, such as a safe harbor framework for cloud computing, also are worthy of consideration.

Second, we recommend that the final Regulation permit the free transfer of depersonalized data in cloud computing applications. Recitals 23 and 24 of the proposed Regulation in fact support this recommendation. Statements in these recitals provide that "the principles of data protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable" and that "identification numbers or online identifiers need not necessarily be considered personal data in all circumstances." The definition of personal data, which relies on the definition of "data subject," further supports these statements as it must be possible to identify an individual by means of the data itself. Where sufficient security measures, such as strong encryption, are taken to ensure the depersonalization of the data, the processing of that data in cloud computing applications would be consistent with general data protection principles.[13]

---

[12] The Article 29 Working Party Cloud Computing Opinion focuses on the location of all servers being within the EU. Art. 29 Working Party Cloud Computing Opinion. However, this ignores the importance of the cloud computing provider having sufficient markets and efficiencies to remain financially viable, a factor that is key to availability, portability, and accountability. The requirements of confidentiality and data security and the proprietary nature of how a company establishes its cloud all support a policy that does not require disclosing the locations of all servers.

[13] Even if data in the cloud are not encrypted, acknowledging the concept of sharding as an accepted compliance means should be considered. See, W. Kuan Hon, Christopher Millard & Ian Walden, *The Problem of 'Personal Data' in Cloud Computing – What Information is Regulated? The Cloud of Unknowing, part 1*, Queen Mary University of London, School of Law, Legal Studies Research Paper No. 75/2011 (updated April 13, 2011), available at http://www.cloudlegal.ccls.qmul.ac.uk/Research/researchpapers/45905.html). "Sharding" or fragmentation is an automated procedure performed by a cloud provider's software, which automatically breaks up data into fragments for storage in different storage equipment, which can be in different locations. This is similar to the example used by the ICO for anonymization through use of reference numbers where the controller maintains the key that links the reference number to the individual. *See*, United Kingdom Information Commissioner's Office, *Draft Anonymisation Code of Practice* (for consultation, 31 May 2012-23 August 2012), 16, available at http://www.ico.gov.uk/about_us/consultations/~/media/documents/library/Corporate/Research_and_reports/anonymisation_cop_draft_consultation.ashx.

5. Conflicting Legal Obligations

The Draft Regulation functions as a standalone regulatory regime. That is, the interpretation and implementation of the proposed prohibitions and requirements are governed almost completely by its own terms. In practice, however, persons and enterprises that necessarily process and use personal information face a wide range of legal and regulatory obligations and prohibitions that may conflict with those imposed by the Draft Regulation. We are concerned that the Draft Regulation does not adequately address these sometimes irreconcilable conflicts by recognizing that privacy imperatives in some circumstances may, or even should, be outweighed by countervailing legal and policy considerations. Global enterprises must, by necessity, store and process data on European nationals to complete routine and expected business relationships. Moreover, non-privacy laws and regulations mandate or contemplate that this information be used to discharge legal obligations they impose. Therefore, reconciling the requirements of the Draft Regulation with overlapping regimes eventually will become necessary. The Sections believe that this issue should be addressed in the Draft Regulation itself and not be left to uncertain and uneven resolution over time. Specifically, to the extent the Draft Regulation does not entertain exceptions or derogations that recognize these conflicting legal obligations, persons and enterprises subject to coverage by the Draft Regulation could find themselves in the unfavorable position of choosing to violate one or the other of those obligations.[14]

We offer the following examples to illustrate the conundrum:

- Anti-bribery laws (including the United Kingdom Bribery Act and the United States' Foreign Corrupt Practices Act) obligate parties to conduct meaningful investigation upon suspicion that a party's employee may have engaged in corrupt activity. The adequacy of the subsequent internal investigations is both critical to the detection of public corruption and material to any penalties that may be imposed. By definition, advance express consent to investigate previously unsuspected unlawful activity is implausible. Absent an appropriate exception to permit confidential investigatory processing a party may find itself forced to choose between conflicting legal obligations. In antitrust investigations, without this type of exception a party may be inhibited from seeking amnesty, which is a particularly unfortunate effect for enforcement of these laws.

- Employers are broadly required to maintain data on their current and former employees for tax, pension, employee benefits and other reasons. To the extent that the Draft Regulation's "right to be forgotten"[15] applies other than to on-line social media settings (a plausible interpretation of the Draft Regulation), compliance with an employee's (or former employee's) request that their data be deleted once again puts that employer in a position of choosing between conflicting legal obligations.

[14] Given the substantial monetary fines introduced by the Draft Regulations, the dilemma is far from hypothetical.

[15] See discussion below at Section 6 of these comments.

- Data controllers in the financial services industry face anti-money laundering, fitness, probity and other legislative and administrative regulatory requirements that necessitate the retention and use of personal data, including sensitive personal data, in a manner that potentially conflicts with the requirements of the Draft Regulation.

- Where, as in the United States, private litigation carries with it discovery obligations, parties and their counsel may be required to preserve and produce data that consist of or contain sensitive personal information. Discovery obligations also may arise within the EU Member States, particularly in the United Kingdom. Discovery is not optional, and failure of a party or counsel to comply with discovery or document retention obligations may result in severe penalties up to and including sanctions for contempt of court. The mere search for and retrieval of personal data may itself conflict with the party's obligations under EU privacy law, and the transmission of that data to a non-EU jurisdiction in compliance with discovery requests or orders also may violate prohibitions on data transfers to non-community jurisdictions. Likewise, document retention obligations incident to the discovery process may conflict with a right to be forgotten if that right remains in the Draft Regulation.

We do not suggest that it is either possible or feasible to include in the Draft Regulation a full list of every current or conceivable conflicting legal obligation and a resolution of that conflict. Nor do we suggest that privacy concerns always should be subordinate to or limited in the face of these conflicting legal obligations. Rather, we suggest that the Draft Regulation explicitly recognize that clearly applicable and conflicting legal obligations or prohibitions provide a recognized and sanctioned legal basis to access and process existing data to the extent, and only to the extent, necessary to discharge or comply with those obligations where a party is not able to avoid or limit the data requirements of the conflicting legal regime by reference to or reliance on EU privacy law. We believe such a mechanism provides a satisfactory means to reconcile conflicting legal requirements without sacrificing the privacy or security of EU data subjects.

6. Right to be Forgotten

The Draft Regulation's proposed recognition of a right to have one's data expunged from digital memory, even where that data is accurate and was voluntarily provided by the data subject in the first instance, is an innovative development. The Sections recognize and acknowledge the desire to maintain data subjects' control over the downstream uses of their information, particularly where such use may not have been anticipated when the data first was provided. However, the current articulation of this new right may create substantial unintended consequences.

The Draft Regulation itself incorporates the concept of proportionality.[16] Data controllers have many legitimate reasons to process data (or have it processed for them), and to maintain

[16] "The principle of proportionality requires that any intervention is targeted and does not go beyond what is necessary to achieve the objectives." Draft Regulation, Explanatory Memorandum at p. 6.

that data for effective and accurate processing and use. These data controllers thus have legitimate and compelling reasons to retain personal data, a need that we suggest should be balanced with the requesting individual's desire to be forgotten. The Sections suggest that describing the right to be forgotten in absolute terms may well have adverse consequences. These may include:

- Denial of individual benefits (e.g., post-termination or retirement benefits administration could be hampered if a former employee has a virtually unilateral right to be forgotten with regard to human resources records)

- Denial of an individual's ability to enforce legal rights (e.g., if a group of female employees believe they are unfairly compensated based on their gender, but a handful of female employees has invoked their right to be forgotten and their compensation and benefits records were deleted, then the group of women, the employer, and the courts may be denied the ability to accurately evaluate and resolve the claim).

- Facilitating illegal activity (e.g., in cases of fraud the victim may be unaware of the alleged crime and thus unable to request retention of relevant records in a time frame suitable to pursue a claim, a problem exacerbated by the perpetrator's conceivable ability to request erasure of records that may be relevant but that include personal data about the perpetrator).

- Endangering health and safety (e.g., in the case of clinical trials, an individual's adverse reactions or other medical outcomes are of paramount importance to both the development of effective pharmaceuticals and other treatments and to the safety of persons participating in the trial).

- Impeding the advancement of legal defenses (e.g., business records very often include personal data and those records may be relevant to establishing legal compliance or mounting a legal defense; deletion of those records based on individuals' privacy concerns may deprive a business of its ability to demonstrate compliance or to defend allegations of noncompliance, and similarly may deny authorities a full and fair view of the merits of a claim).

Acknowledging the legitimate goal of enabling data subjects to maintain appropriate discretion with regard to the subsequent use of their personal information, the Sections recommend that the decision to accord the principle the status of a right be re-examined. We believe that the protection against permanent and unwanted use can be achieved more effectively by replacing the right to be forgotten with a set of principles that balance individuals' interest in limiting permanent use of their data with the legitimate needs of those to whom they provided their data in the first place. This principle-based approach is consistent with existing EU privacy law, and would provide the vehicle for balancing the otherwise incompatible interests of data subjects and controllers. As with other principle-based obligations (such as those for data integrity, consent and the like), the data controller would be provided clear guidance as to the conditions under which it may process or use personal information, but would not face the kind of absolute prescription that may not fully serve other, equally valid interests that favor (or even

require) the retention of data. We believe the concerns of data permanence that undergird the proposed right to be forgotten can be fairly met by application of a "restricted processing" option.[17]

7. Data Breach Notification

The Sections support the adoption of a data breach notification requirement. Articles 31 and 32 of the Draft Regulation provide for notification of a breach to the appropriate supervisory authority and, in certain circumstances, to the affected data subjects as well. In the United States, there is no federal data breach notification requirement of general applicability, but virtually all of the individual states have enacted notification statutes. While these statutes vary from state to state and could benefit from national harmonization, they have created an appropriate mechanism and effective motivation for those with knowledge of a data breach to make appropriate disclosures to affected parties and, in some instances, law enforcement authorities. Indeed, the imposition of this obligation has resulted in data controllers imposing data security and breach notification obligations by contract on their service providers, extending the effective scope of the benefit that notification laws provide.

The Sections, however, suggest modification of two provisions of the Draft Regulation's breach notification requirement. First, as drafted, Article 31 requires that the supervising authority be notified of the breach within twenty-four hours after the data controller first becomes aware of the fact of the breach, if "feasible." That notification must not only disclose the fact of the breach, but also must (1) include information as to the categories of data lost or misused, the number of the data subjects involved, and the number of data records exposed; (2) describe the mitigating steps that will or should be taken in response to the breach; (3) describe the "consequences" of the breach; and (4) otherwise describe the breach in all of its detail and possible effect.

Based upon extensive experience in the United States with data breach notification regimes (and the experience to date of mandatory reporting by telecommunications providers and Internet service providers under the EU's E-Privacy Directive), the Sections believe that very seldom (if ever) will it be feasible to conduct an adequate investigation, compile all relevant information, diagnose the cause of the breach and plan appropriate mitigation within a single day. In fact, our experience is that the first day following discovery of a potential breach provides only enough time to *begin* an appropriate investigation. Imposing a premature notification obligation not only is likely to yield mostly useless notification, but may actually interfere with the process of discovering the true nature of a suspected breach.

[17] The concept of "restricted processing" in lieu of erasure is acknowledged in Article 17 of the Draft Regulation, but is limited to four specific situations that do not fully address many of the examples provided above of certain challenging situations where the rights and duties of natural persons or legal entities may be implicated. Those four situations are: (1) data subject challenges accuracy of data (in which case restricted processing is permitted only for so long as necessary for controller to confirm accuracy; (2) for purposes of proof; (3) if processing is unlawful but data subject requests restricted processing rather than erasure; (4) data subject requests a transfer of the data to another automated processing system in accordance with proposed Article 18. If any of these four scenarios apply, the Draft Regulation provides that restricted processing must include only storage and "process[ing] for purposes of proof, or with the data subject's consent, or for the protection of the rights of another natural or legal person or for an objective of public interest." While this latter concept addresses some of the concerns expressed in these comments, the concepts are not available to data controllers unless one of the aforementioned four circumstances has occurred, meaning that the overall concept of restricted processing acknowledged in the proposed regulation is helpful, but so rarely available that it will not, as currently structured, address the concerns raised in these comments.

Accordingly, the Sections recommend that the initial notification deadline be set in such a way as to permit and encourage an investigation and planning process that realistically takes into account the challenges faced by any entity that suffers a data loss. Many existing data breach laws require that notification be made as expeditiously as reasonably possible and without unreasonable delay, recognizing the time necessary to secure the affected systems and to cooperate with law enforcement authorities. These notification regimes have proven both effective and flexible, and experience commends this approach. If the Draft Regulation does include a stated period of days for the notification, our experience is that anything shorter than fifteen days is not generally feasible, and thirty to forty-five days may be more typical in well-functioning breach notification systems.

Our second concern is similar to that raised above regarding the reliance placed on delegated acts and implementing provisions. These delegated acts could result in inconsistent obligations for what must be included in the notice and the form of notification. Our experience in the United States with a decentralized approach to the type of notification and the content of the notice is that it can slow down the notification process and delay effective notice to affected data subjects. Moreover, it is important to ensure the availability of a recognized alternative means of notification when individual content information is not available, which is frequently the case in credit card data breaches. We recommend that both the method of notification and the content of the notice be consistent throughout the EU.

8. Monetary Penalties

Article 79 of the Draft Regulation authorizes imposition of administrative sanctions by a supervisory authority for violations of the Regulation. In most cases, these sanctions take the form of fines, which increase according to the relative seriousness of the violation. The fines authorized by the new Article 79 differ from those authorized by Article 24 of the existing Data Protection Directive in that they are more specific and prescriptive, their amounts are not determined at the Member State level, and the prescribed amounts are markedly higher than the fines imposed by the Member States under the existing Directive.

The Commission states its intention to establish fines that are "effective, proportionate, and dissuasive." Notwithstanding this understandable goal, the Sections recommend several clarifications to Article 79, which we believe would better serve to advance the aims of the Commission, and ultimately, the care given to data privacy and protection in the EU.

We first recommend that the Commission, while maintaining a firm ceiling on potential fines, provide greater discretion to a supervisory authority to determine when a fine is appropriate and, if so, what amount should be assessed. The Draft Regulation advises the imposition of the same fine on a person who, in good faith, provides the required information to a data subject but in the wrong format as it would upon a person who blatantly disregards a more substantive prescription or proscription of the Regulation. By allowing a supervisory authority to judge the merit of each case using the provisions contained in Article 79 more as a guidelines than as a list of structured prescriptions, the supervisory authority will be better able to isolate the true culprits from those that simply make minor missteps while giving their best efforts to achieve compliance with the Regulation.

More specifically, we suggest that the mandatory "shall impose" be replaced with a discretionary "may impose" in Article 79(4), (5), and (6). By insisting that the supervisory authority "shall impose" fines for each and every case of technical noncompliance, the Draft Regulation would require persons to be fined a potentially large sum for noncompliance even in instances in which there is no demonstrable negative consequences for any data subject. As an example, under the Draft Regulation a supervisory authority would be required to assess a fine of up to two percent of an entity's global annual revenue for failing to "timely" or "completely" notify the supervisory authority of a data breach. It is easy to foresee instances in which "timely" or "complete" notification is not made due to human error or lack of information, but in which this less-than-perfect notification presents no real or material threat to the concerned data subject.

Additionally, from an administrative perspective it would be impractical for a supervisory authority to impose fines in every instance of noncompliance. Were the supervisory authority to attempt to do this, it would quickly expend its limited resources and thus be in position where it is less able to enforce violations that have a real impact on data subjects.

Because of the relatively large size of available fines, and given the lack of any warning provided to persons not included within Article 79(3)(b), we also recommend that the maximum amount of the fines be reduced and that they initially begin at a much lower threshold and increase according to a multiyear schedule thereafter. This will allow concerned persons the opportunity to become familiar with how the mandates of the Regulation will be enforced in practice before they become liable for fines that could amount to hundreds of millions of Euros.

In addition, there are two points on which further clarification would be beneficial. First, with respect to the fine-assessment practices of the supervisory authorities we suggest clarification as to whether or not certain fines assessed against persons would be subject to the requirements of Article 58(2), which provides that the European Data Protection Board review any action taken by a supervisory authority that is "intended to produce legal effects" and that is made in connection to "processing activities which are related to the offering of goods or services to data subjects in several Member States," among other activities. From a plain reading of the Draft Regulation, it would appear that a fine assessed against a person operating in multiple Member States could be included in the ambit of this mandatory review. We would welcome this interpretation, as it would more closely connect the important oversight provided by the European Data Protection Board to the imposition of fines by the supervisory authority, as well as serve to enhance the consistency of the Regulation, which is a stated goal of the Commission throughout.

Second, with respect to the authority to impose fines, Article 79(1) states that "each supervisory authority shall be empowered to impose administrative sanctions." We interpret this to mean that each supervisory authority is empowered to impose fines only against persons under its jurisdiction pursuant to Article 51(2), and that a person would not therefore be subject to fines imposed by multiple supervisory authorities for single occurrence of non-compliance that may implicate data subjects in more than one Member State. If this understanding is incorrect, we recommend that the language of the Article 79 be revised to state that a person can only be assessed a fine by one supervisory authority for any one violation, or series of related violations, even if these instances occur across multiple Member States.

* * * *

The Sections appreciate the opportunity to provide these comments to the Draft

Regulation and hope that the Commission finds them useful.

Respectfully submitted,

Section of Antitrust Law

Section of International Law

American Bar Association