September 5, 2012

Jan Philipp Albrecht
Rapporteur, Committee on Civil Liberties, Justice and Home Affairs
European Parliament

Lara Comi
Rapporteur, Committee on Internal market and Consumer Protection
European Parliament

Re: European Commission General Data Protection Regulation

Dear Mr. Albrecht, Ms. Comi, and Members of the European Parliament,

We are writing to you on behalf of consumers in the United States in support of the new European Union privacy law. For many years, US consumer organizations have urged policy makers to improve data protection laws and protect the privacy rights of consumers. This focus is understandable, as a glance at newspaper headlines reveals many examples of identity theft, data breaches, invasive government surveillance, broken privacy promises, and the profiling of Internet users. "Cloud computing" has raised fundamental questions about who will access and control detailed consumer data that is obtained for new Internet-based services. In response to the developments in the digital environment, the European Commission has proposed a new Regulation on the protection of individuals with regard to the processing of personal data, the "EU General Data Protection Regulation," which you are now reviewing on behalf of the European Parliament,

We support the EU General Data Protection Regulation and believe that it provides important new protections for the privacy and security of consumers. Moreover, we believe that the promotion of stronger privacy standards in Europe will benefit consumers around the globe, as businesses improve their privacy practices and security standards. Indeed, it is clear that the adoption of the EU Data Protection Directive in 1995 had this effect. This "ratcheting up" effect for consumer protections is a key reason that consumer organizations around the world support efforts to strengthen privacy safeguards within the European Union.

The Challenge of Privacy Protection

In the digital environment, consumers face a wide range of threats to the privacy and security of their personal data. Social network firms now store information about nearly every facet of a consumer's life. Government agencies and private companies increasingly collect biometric information through technologies such as facial recognition. Private companies unilaterally change the terms that govern the handling of personal data. Advertising networks track consumers as they browse the Internet. Data brokers develop detailed profiles of consumers and then sell these profiles without the knowledge or consent of the consumers involved. And

government intelligence agencies conduct invasive electronic surveillance with little oversight, often relying on customee data acquired from Internet companies.

Polls make clear that consumers are very concerned about these developments, and policymakers in the United States and Europe have proposed several new frameworks to address these challenges. In the United States, the Obama Administration proposed a "Consumer Privacy Bill of Rights" that contains the basic elements for privacy protection, though this framework still has no legal force[1] The US Federal Trade Commission published "Protecting Consumer Privacy in an Era of Rapid Change," which also proposes basic safeguards for consumers [2] Earlier this year, the European Commission set out the General Data Protection Regulation with the expectation that it will become law after a process of consultation and review.[3] The Regulation addresses the new challenges faced by consumers in the digital environment, and provides a uniform framework for European data privacy.

Summary of the European Privacy Regulation

The General Data Protection Regulation ("GDPR") addresses these challenges through several important provisions.

- The GDPR expands the definition of personal information to reflect the new ways that data may be linked to individual consumers (Art. 4)
- The GDPR strengthens the requirement of meaningful consent (Art. 7).
- The GDPR emphasizes transparency in data practices as well as data minimization (Art. 5)
- The GDPR improves the ability for consumers to gain access to the information about them that is collected by businesses (Arts. 12, 14)
- The GDPR establishes a new right to limit profiling (Art. 19).
- The GDPR promotes Data Protection by Design and by Default, as well as Privacy Enhancing Techniques. (Art. 23)
- The GDPR establishes a broad data breach notification requirement. (Art. 31).
- The GDPR creates a new responsibility to undertake Data Protection Impact Assessments. (Arts. 31, 33-34)

---

[1] http://www.whitehouse.gov/sites/default/files/privacy-final.pdf. The CPBR contains seven principles: (1) individual control over the collection and use of personal data; (2) transparency; (3) respect for the context in which data is collected; (4) security; (5) access and correction rights for consumers; (6) data limitation; and (7) accountability.

[2] http://www.ftc.gov/os/2012/03/120326privacyreport.pdf. The FTC report focused on three principles: (1) privacy by design, (2) choice, and (3) transparency

[3] http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

- The GDPR strengthens the independence and authority of data protection agencies. (Arts. 46-54)

- The GDPR strengthens the remedies and redress rights of consumers (Arts. 73-79)

- The GDPR affirms the importance of Freedom of Expression, particularly for journalistic, artistic and literary expression. (Art. 80).

- The GDPR acknowledges the importance of scientific, historical, and statistical research. (Art. 83).

These new provisions update the principles of the 1995 EU Data Protection Directive to new business practices, and help restore consumer control over personal data. The protections contained in the Privacy Regulation implement the basic human right of the individual to autonomy and control of personal information. Furthermore, by protecting against abusive data practices, security breaches, and identity theft, the Privacy Regulation will increase trust and confidence in the digital marketplace. The Regulation also adopts several innovative approaches to privacy protection, such as privacy by design and privacy by default, that take advantage of new techniques to safeguard consumer privacy.

And the Regulation helps to better coordinate the various European data protection regimes. (Arts. 55-72) The system establishes single, national data protection authorities in each member state, which monitor and ensure the application of the Regulation, certify companies, authorize binding corporate rules, and hear and investigate complaints lodged by the data subject. When a data protection authority adopts a measure that affects more than one member state, the authority will submit a draft measure to the Commission and the European Data Protection Board for approval.

Regarding "the right to be forgotten," this principle seeks to hold major Internet firms accountable for the data on users they collect and make available to the public for profit. It builds on the right to data deletion, a critical element of data protection, that needs to be strengthened in light of the reluctance of firms to make clear what data they possess, how it is used, and what rights consumers have when they seek to end a service relationship. Internet speech about public figures or issues of public concern should be protected.

Recommendations from US Consumer Organizations

Before being adopted, we understand that the Data Protection Regulation will pass through a series of revisions and negotiations among the Member States. The revision process provides an opportunity for further strengthening and clarifying the GDPR. Based on our experience with several matters in the United States, we would recommend:

- *Narrowing the scope of the general exceptions*: Although the Regulation applies to the processing of personal data in general, several exceptions exist. In order to foster uniform application, the scope of these exceptions should be better defined.

- *Narrow the scope of the "legitimate interests" exception for data processing*: The Regulation allows for data processing "for the purposes of the legitimate interests pursued by a controller." Although the exception is subject to a balancing test, the definition of "legitimate interests" represents a possible "catch-all" category apart from consent, contracts, legal obligations, vital interests or public interests. In order to prevent "legitimate interests" from becoming a loophole, the definition of the term should be clarified.

- *Strengthen the right to data portability:* The Regulation provides for both the right to erase personal data and the right to transfer data from one processor to another. The Regulation should clarify that transfers of personal data under the right to data portability entails the deletion of data by the original service provider. Furthermore, there should be limits on the ability of business to condition the provision of services on consumers porting their data to that service.

- *Promoting greater transparency in data practices, particularly regarding the profiling and "scoring" of consumers*: The Regulation protects individuals from profiling designed to "predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behavior." The Regulation should provide consumers with the right to know whether they are being profiled, to obtain a copy of their profile, and to obtain specific information about the specific techniques and numeric values associated with the profiling.

- *Restricting the circumstances for "blanket" consent*: The conditions for consent specified in Article 7 could allow for the possibility of a single, "one size fits all" consent provisions that purport to represent consent to data processing in perpetuity. Such a mechanism is not meaningful if consumers (and even the businesses) do not know which future acts the consent would enable. The Commission should clarify whether this method of obtaining consent satisfies the Regulation.

- *Include non-economic loss in the context of data breach notification*: The Regulation provides for notification to affected consumers of data breaches when the breach is likely to "adversely affect" the consumer. The Commission should clarify that "adversely affect" includes harms beyond economic loss, such as reputational or psychological harm.

- *Ensure that codes of conduct and certification schemes do not become weaker versions of legal rights*: The Regulation encourages the development of self-regulatory codes of conduct by data controllers and processors, and provides for cooperation with other jurisdictions attempting different protection frameworks. The Commission should ensure that these self-regulatory approaches do not become a means of circumventing the more protective standards of the regulation itself.

Conclusion

The efforts in Europe to strengthen and update the basic legal framework for privacy protection provide several lessons for US policymakers. As the Transatlantic Consumer Dialog has previously stated, "the EU Data Directive is a concise statement of principles that make clear to business and consumers what their rights and obligations are." The TACD noted that the EU approach to privacy protection tends to be "technologically neutral, focusing on the collection and use of personal information and not the specific technologies involved." TACD also emphasized that the EU approach "seeks to make business practices more transparent so that consumers can make more informed decisions in the marketplace."

We believe that this approach, which sets out rights and responsibility for the collection and use of personal data, is the cornerstone of data protection in the modern era.

We support the enactment of the General Data Protection Regulation. Consumers on both sides of the Atlantics have made clear that privacy protection is a critical concern. The Regulation will advance the protection of privacy in both Europe and the United States. We look forward to working with you on this important undertaking.

Sincerely,

Advocacy for Principled Action in Government
Center for Digital Democracy
Center for Media and Democracy
Consumer Action
Consumer Federation of America
Consumer Watchdog
Consumers Union
Cyber Privacy Project
Electronic Privacy Information Center
Essential Information
The FoolProof Initiative
Friends of Privacy USA
Liberty Coalition
National Association of Consumer Advocates
National Consumers League
Patient Privacy Rights
Privacy Journal
Privacy Rights Clearinghouse
Privacy Rights Now
Privacy Times
Public Citizen
U.S. PIRG

REFERENCES

Proposal for a Regulation of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and the free movement of such data (General Data Protection Regulation), E.C. COM (2012) final, (Jan. 25, 2012) http://ex.europa/eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

EPIC, "EU Data Protection Directive" http://epic.org/privacy/intl/eu_data_protection_directive.html

European Consumer Organization (BEUC) Position Paper: Proposal for a Regulation (July 27, 2012), https://epic.org/privacy/BEUC-Position-Paper.pdf

The Public Voice, "Madrid Privacy Declaration" (2009) http://thepublicvoice.org/madrid-declaration/

TACD Resolution: Consumer Privacy Rights (May 24, 2012), http://tacd.org/index2.php?option=com_docman&task=doc_view&gid=343&Itemid=40

TACD Letter to US Congress on Hearing: "Internet Privacy: The Impact and Burden of EU Regulation" (Sept. 14, 2011), http://tacd.org/index2.php?option=com_docman&task=doc_view&gid=329&Itemid=40

TACD Resolution: Behavioral Advertising (June 21, 2011), http://tacd.org/index2.php?option=com_docman&task=doc_view&gid=298&Itemid=40

TACD Resolution: Cloud Computing (June 21, 2011), http://tacd.org/index2.php?option=com_docman&task=doc_view&gid=296&Itemid=40

TACD Resolution: Core Consumer Protection Principles in Electronic Commerce (Sept. 1, 1999), http://tacd.org/index2.php?option=com_docman&task=doc_view&gid=135&Itemid=40

The White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy 1-2 (2012) available at <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>.