EUROPEAN COMMISSION
DIRECTORATE-GENERAL JUSTICE AND CONSUMERS

Directorate C: Fundamental rights and rule of law
Unit C.4: International data flows and protection

Brussels, 9 November 2018
JUST.C.4/CM

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW
Room 4725, Attn: Privacy RFC
Washington, DC 20230

Submitted by e-mail to: privacyrfc2018@ntia.doc.gov

Subject: Request for public comments on a proposed approach to consumer privacy [Docket No. 180821780-8780-01]

Dear Assistant Secretary Redl,

We have read with great interest the recent publication and request for public comments by the National Telecommunications and Information Administration (NTIA) of the U.S. Department of Commerce on proposed privacy outcomes and high-level goals for Federal action on consumer privacy.

The EU and the United States have a very close relationship and long-standing cooperation in a number of areas that increasingly rely on transatlantic data flows, including trade, regulatory and law enforcement cooperation. A common set of data protection principles has already been agreed between the EU and the United States in both the commercial field (the "EU-US Privacy Shield" framework[1]) and the law enforcement area (the "Data Protection and Privacy Agreement" or "DPPA"[2]). In building on these principles and increasing convergence between our approaches towards data protection, we can help to facilitate data exchanges while further strengthening these instruments.

Against that background and given that, in the past years, the EU has gone through a similar process of consulting stakeholders and reforming our privacy rules, we appreciate

[1] See Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield.

[2] Agreement between the EU and the U.S. on the protection of personal data when transferred and processed for the purpose of preventing, investigating, detecting or prosecuting criminal offences, including terrorism, in the framework of police cooperation and judicial cooperation in criminal matters (in the EU referred to as "Umbrella Agreement").

the opportunity to submit the comments below. We understand that this consultation covers only the first step in a process that might lead to Federal action and would therefore like to express our readiness to provide further comments on a more developed proposal in the future.

In our view, and as increasingly accepted globally, the basic architecture of a modern, balanced and flexible privacy regime is characterised by four key elements: an overarching law; a core set of data protection principles; enforceable individual rights; and finally, an independent supervisory authority with effective powers to ensure the enforcement of those rules. We welcome that these elements are also at the core of NTIA's proposed approach to consumer privacy, and have therefore structured our comments broadly around those four aspects:

- First, we note that one of the high-level goals identified by NTIA is the **harmonisation of the regulatory landscape** through a set of overarching principles that would apply to all business activities previously not covered by sectoral laws. Given the considerable increase in the use and exchange of data, including personal information, across all sectors of the economy – with the consequence that sectoral laws thus cannot provide the necessary legal certainty to business organizations nor ensure the necessary protection of consumers – this would be significant progress. Overcoming the current regulatory fragmentation would create a level playing field, ensuring that data can move easily between operators, industries and business models on the basis of clear and harmonised rules while guaranteeing a consistent protection of individuals. In line with the existing sectoral rules and as a reflection of the fundamental value of privacy, we believe that these comprehensive principles and safeguards should be enshrined in a legislative instrument and not be left to soft law instruments or self-regulation. Doing so does not affect the necessary flexibility as statutory rules still leave space for further clarification through interpretative guidance, taking into account lessons learnt and technological developments.

- Second, we fully share the view of NTIA that **trust** should be at the core of the U.S. (and in fact any) privacy policy formulation. We strongly believe that, giving individuals more control over their own data will increase trust in the way businesses handle their data, with the result that individuals will be more willing to share their information and use services. This trust, particularly in the online environment, is essential to support the development of the digital economy. Conversely, if individuals are afraid that others will not respect their privacy or fail to guarantee the security of their data, they will lose confidence and become averse to certain forms of online activities. Ensuring trust should therefore guide the development of all data protection principles and safeguards.

- Third, we very much welcome that the seven user-centric privacy outcomes proposed by NTIA cover **core data protection principles** that have been developed since the 1970's and are now widely shared across the world. For instance, the principles of "reasonable minimization", "security", "transparency" and "accountability" are essential safeguards but also reflect sound data management (and thus good business practice). At the same time, we note that certain other core principles are currently not explicitly reflected in NTIA's proposed privacy outcomes. These include for instance the principle of **lawful data processing** (i.e. the need for a legal basis), the requirement to process personal data only for **specific purposes** (and further process it for purposes that are not incompatible with the original purposes), a central reference point also for other principles (e.g. that of limited data retention); the requirement that

personal data should be **accurate** and **relevant** for the purposes for which they are processed; and specific protections for **"sensitive data"** (i.e. personal data for which there is a particularly high risk that they could become grounds for discrimination, e.g. religious beliefs, sexual orientation or health conditions). These principles are not only widely accepted as key elements of modern data protection legislation, including to ensure individuals' greater confidence in the way their data are collected and handled, but have also been codified in important recent instruments agreed between the EU and the United States.[3]

- Fourth, in our view, **effective safeguards and enforceable individual rights** are key components of a modern data protection regime.

  We therefore very much welcome that, according to the RFC, the desired outcome of consumer privacy in the United States would revolve around the information and empowerment of the consumer, in particular by ensuring **transparency** and **control** of his/her data. Individuals should be clearly informed about what happens to their data (what data is processed, for which purposes, who is processing the data, with whom might it be shared, etc.), including in case their data is stolen or lost (data breach). In this respect, since these incidents can have very harmful consequences (identity theft, fraud, etc.) it might be useful to include a requirement to **report data breaches**. This is a key safeguard enabling individuals to protect themselves from (or at least mitigate) potential harm already recognised for instance in the DPPA (Article 10). While we understand that data breaches laws have been enacted by States, businesses and individuals could benefit from the harmonisation of the conditions for the notification of such incidents.

  Putting individuals in control of their personal data also presupposes that they benefit from a clear set of enforceable rights to effectively exercise such control. In this regard, we welcome the inclusion in the RFC of core data protection rights such as the right to access and correction. In addition, with a view to addressing particular challenges of the digital world, it might be worth considering going beyond those 'classic' rights. For instance, there is a need to specifically protect individuals when they are significantly impacted by decisions based solely on automated processing (e.g. the rejection of an online credit, or an e-recruiting application). **Automated individual decision-making** and profiling have great potential to speed up decisions, make them more informed and objective. At the same time, they can also pose risks for individuals, for instance if the underlying algorithms are 'biased'. Given the increasing relevance of the use of algorithms in data processing, the 'traditional' rights of access, correction and erasure might be insufficient to ensure effective control of individuals over their data and protect them against discrimination. Therefore, while we understand that certain protections already exist in sectoral laws, we would recommend considering a requirement to explain the underlying logic of automated decisions and a right for individuals to ask for such decisions to be reviewed by a human being when such decisions can have legal effects or otherwise significantly affect them. Again, this is a right already recognised for instance in the DPPA (Article 15).

[3] See for example the Choice, Data Integrity and Purpose Limitation Principles (Privacy Principles 2, 5) of the EU-US Privacy Shield and Articles 6, 8, 12, 13 and 15 of the DPPA.

Last but not least, a key data protection safeguard is to empower individuals to pursue **legal remedies** to effectively enforce their rights, in a timely manner and without prohibitive cost. This includes the right to lodge a complaint and have it resolved[4] as well as the right to effective judicial redress. Given the fundamental importance of data protection as a reflection of human dignity and an element of individuals' autonomy and self-determination, obtaining redress should not be subject to restrictive requirements or burdensome conditions, for instance in terms of harm.

- Fifth, the effective implementation of privacy rules crucially depends on **robust oversight and enforcement by an independent authority**.

  In this respect, we welcome the emphasis by NTIA on enforcement by the FTC, including the importance of having the necessary resources, clear statutory authority and direction to enforce consumer privacy. We also note that the FTC has initiated a process of reflection on its current authorities in the area of privacy, which notably looks into the efficacy of the FTC's use of its current remedial authority and the need for any additional tools or powers to adequately deter unfair and deceptive conduct related to privacy and data security. One of the lessons learned from recent scandals about the mishandling of personal data is that we need to get serious about oversight and enforcement, especially as some violations of privacy laws can have particularly negative consequences for individuals and, where they affect the democratic process, society as a whole. Strengthening the **FTC's enforcement role** would also reinforce the foundations of the Privacy Shield, a key instrument that facilitates transatlantic data flows.

  Moreover, in our view, it would be important to consider the introduction of affordable mechanisms (provided, for example, in the EU through the role of data protection authorities) ensuring the **effective resolution of individual complaints** that might not necessarily correspond to the FTC's enforcement priorities at any given moment (e.g. because of their limited importance from a strategic point of view, even if the alleged violation might be very relevant for the individual complainant). The existence of such mechanisms could significantly contribute to consumer trust, while ensuring quick resolution of disputes and thus preventing lengthy and costly litigation.

  Finally, while we fully agree with the importance of a strong culture of "accountability", we equally believe that, to be credible, a system based on the own responsibility of business operators should be coupled with robust enforcement in case of non-compliance. This includes, as in other areas of law, putting in place credible and sufficiently **deterrent sanctions**.

[4] See for instance the EU-US Privacy Shield, which requires certified U.S. companies to respond to individuals within a fixed period of time and to "*address whether the complaint has merit and, if so, how the organization will rectify the problem*" (Supplementary Principles 11.c. and 11.d.i.). If the individual is not satisfied with the reply, (s)he can seek redress with one of the available "*independent recourse mechanisms by which each individual's complaints and disputes are investigated and expeditiously resolved at not cost to the individual*" (Privacy Principle 7.i.).

Looking at the overall approach, we share the NTIA's view that data protection rules must not stifle innovation and that strong protections, legal clarity and flexibility are all important elements of a modern privacy regime.

In our experience, **privacy and innovation** are two complementary objectives, rather than mutually exclusive. Data protection rules, if designed properly, can in fact encourage innovation, for example by guaranteeing that data protection safeguards are built into products and services from the earliest stage of development (data protection by design and by default). This incentivises businesses to innovate and develop new ideas, methods and technologies for security and the protection of personal data. We therefore very much welcome the NTIA's emphasis on incentivizing privacy by design and, more generally, privacy research.

We note that NTIA's approach focuses on "*the outcomes of organizational practices, rather than on dictating what those practices should be*." In this respect, we certainly agree that data protection rules should normally not prescribe specific ways of data processing but rather ensure that such processing complies with certain principles and respects certain safeguards. In addition, in our experience a high level of data protection can be applied in a flexible way by making available **different tools to address the broad variety of processing operations** that characterizes the digital economy. This can be achieved by providing for different legal grounds that can be relied upon to collect and process data (not just consent, but also for instance the performance of a contract or legitimate interests of the business operator or third parties). Similar considerations apply for international data transfers: while they should not undermine the level of protection "at home", different instruments can be developed to facilitate such data transfers. In a system based on accountability, this may include elements of co-regulation such as codes of conduct and certification that are 'bottom-up' and can help companies to demonstrate compliance in a way that is adapted to the specific needs and features of their sector or business model.

We also agree on the usefulness of a "**risk-based approach**", which is at the core of NTIA's proposal. As indicated in the RFC under the heading of "scalability", risks are not linked to the size of the business operator, but rather to the type of processing (e.g. volume, categories of personal data handled).

In our view, certain protections can indeed be applied in a flexible way, depending on the level of risk for privacy of the processing operations involved (distinguishing, for instance, between data processing as an ancillary activity and the large-scale processing of sensitive data). In this way, processing operations with limited impact on privacy could be subject to a reduced regulatory burden, thereby also creating incentives to develop innovative, privacy-friendly solutions from the earliest stages of development. However, as privacy is a fundamental value, a certain 'baseline' protection should be ensured regardless of the risks involved. Therefore, we believe that risk assessments should not be applied to all privacy safeguards, but only to additional obligations for business operators beyond that 'baseline'.

More generally, it is important to ensure that "risk-based flexibility" and more generally attention to overall context do not undermine legal certainty and the possibility for both individuals (through private actions) and the competent oversight authority to enforce compliance. Likewise, while the right to privacy and data protection is of course not absolute and reasonable limitations to protect other rights or important public interests

can be justified, we believe that there is a benefit in not tying the level of protection from the outset to broad notions such as "appropriateness" and "reasonableness".

Finally, we welcome that the proposed approach also seeks to contribute to **harmonization and interoperability at global level**. In our view, this can best be achieved through increased convergence, which is, in fact, already a clear global trend as many countries in different regions of the world are putting in place data protection rules that reflect the principles set out in this submission. The same applies for a number of regional instruments, like for instance the Ibero-American Data Protection Standards, as well as the Council of Europe Convention 108[5], the only binding multinational agreement on data protection that already brings together more than 50 State Parties from around the globe. The United States is currently an observer to Convention 108 and should considerer becoming a Party, as it has done with other Council of Europe instruments (e.g. the Cybercrime Convention). Given that companies increasingly operate across borders and prefer to apply a single set of rules in all of their business operations worldwide, joining this global trend would help commercial operators navigate between different legal systems and offer new opportunities to facilitate trade.

We hope that the present observations will be useful for you and we of course stand ready to further explain or discuss these issues.

Yours sincerely,

Bruno Gencarelli
Head of Unit

[e-signed]

[5] Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 180) and 2001 Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (ETS No. 181). On 18 May 2018, the 128th Ministerial Session of the Council of Europe's Committee of Ministers adopted a Protocol (CETS No. 223) amending Convention 108. This Amending Protocol was opened for signature on 10 October 2018.