David J. Redl
Assistant Secretary for Communications and Information
National Telecommunications and Information Administration
United States Department of Commerce
1401 Constitution Avenue NW
Washington, DC 20230

6 November 2018

Docket No. 180821780–8780–01 (Privacy RFC):
Developing the Administration's Approach to Consumer Privacy

Dear Mr Redl,

I represent Brave, a rapidly growing Internet browser based in San Francisco. Brave is at the cutting edge of the online media industry. Its CEO, Brendan Eich, is the inventor of JavaScript, and co-founded Mozilla/Firefox. Brave's employees across the United States innovate in areas such as machine learning, blockchain, and security. We work with partners across the online media and advertising industry.

The National Telecommunications and Information Administration has sought contributions to important questions related to the Administration's approach to consumer privacy. This letter responds as follows.

Key recommendations

1. **A recommendation for a federal law that incorporates the NTIA's intended privacy principles, and draws upon the European model.**
2. **A recommendation to adopt the GDPR approach to "purpose specification", which protects competition and innovative new entrants against anti-competitive data use by large incumbents.**
3. **A recommendation for the United States to build upon GDPR-like standards to maintain global leadership.**

Supplemental points

1. **Accountability requires the concepts of "data controller" and "data processor".**

2. **Notice and consent should not be discounted prematurely.**

This letter also reflects previous correspondence from Brendan Eich, the CEO of Brave, to the US Senate Committee on Commerce, Science, and Transportation, of 28 September 2018, which I enclose herewith for your convenience.

KEY RECOMMENDATIONS

1. A recommendation for a federal law that incorporates the NTIA's intended privacy principles, and draws upon the European model.

The decline in consumers' trust in online commercial services that is revealed in the recently published NTIA/US Census Bureau survey demonstrates the need to act. Successive scandals and breaches demonstrate that self-regulation in the online industry has failed. It is likely that a follow up survey in 2019 will show a far more acute decline.

Therefore, a federal law of an equal or higher standard than state laws is necessary to restore trust and protect the online industry in the United States. We believe that the new framework for privacy regulation in the European Union is the correct model for the such a federal law.

A federal law should, in our view, incorporate the NTIA's intended privacy outcomes (1. transparency, 2. control, 3. reasonable minimization, 4. security, 5. access and correction, 6. risk management, and 7. accountability) as its principles.

It should also incorporate the principles of the General Data Protection Regulation and in Convention 108+ of the Council of Europe. The GDPR and Convention 108+ are the culmination of an exhaustive process of formulation that the United States should exploit to its advantage.

The GDPR and Convention 108+ are closely aligned - and in some cases identical to - privacy principles endorsed by the United States. For example, the NTIA's intended privacy outcomes are incorporated in the GDPR (Article 5), and in Convention 108+ (Article 5). They also incorporate the "Fair Information Practice Principles" of 1973, which were applied to United States federal agencies in the 1974 US Privacy Act; the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal

Data; and the principles endorsed by the United States this year, in Article 19.8 (3) of the new United States-Mexico-Canada Agreement.

Where the principles of the GDPR and Convention 108+ differ from established United States privacy principles is in their explicit reference to "fairness" and "proportionality" as preconditions of data use, a more robust approach to data minimization and purpose specification. In our view, a federal law should incorporate these elements too.

2. A recommendation to adopt the GDPR approach to "purpose specification", which protects competition and innovative new entrants against anti-competitive data use by large incumbents.

From our own experience, we know that the GDPR's burden on small and medium companies has been overstated. In contrast, the restraint that it imposes on incumbents has not been adequately appreciated. As European regulators gradually broaden their enforcement of these new rules, the GDPR's robust approach to purpose specification will help restrain large tech platforms from leveraging their dominant positions in one line of business by cross-using data accumulated in that line of business to dominate other lines of business too.

This is important, because the cross-use of data is a serious antitrust concern. Young, innovative companies can be snuffed by giant incumbents who erect barriers to entry by cross-using data for purposes beyond what they were initially collected for.

Therefore, the robust approach to "purpose specification" taken in the GDPR's "purpose limitation" principle should be a feature of a federal law in order to protect innovative new entrants in the United States market.

3. A recommendation for the United States to build upon GDPR-like standards to maintain global leadership.

The global trend toward GDPR-like standards can support the United States' leading position, provided the United States exploits that trend.

In the coming years, common GDPR-like standards for commercial use of consumers' personal data will apply in the EU, Britain (post EU), Japan, India, Brazil, South Korea, Argentina, and China, for civil and commercial use of personal data. These countries account for 51% of global GDP. Therefore, I propose two items for your consideration.

First, the standard of protection in a federal privacy law, and the definition of key concepts and tools in it, should be compatible and interoperable with this emerging international standard. This includes concepts such as "personal data", opt-in "consent", "profiling", and tools such as "data protection impact assessments", "breach notification", and "records of processing activities". A federal GDPR-like standard would reduce friction and uncertainty, and avert the prospect of isolation for United States companies.

Second, the United States can assume the global lead in this domain by establishing a world-leading regulator that pursues test cases, and defines practical standards. There is a dire need for a well resourced enforcer in the United States, whether in the form of new capacity and powers for the Federal Trade Commission, or a new, separate privacy enforcement agency. Regulators in other jurisdictions are building up their capacity, and the United States needs to compete. For example, by the end of 2018 Ireland will have three times the number of staff examining privacy issues as has the United States (the Federal Trade Commission has only 60 staff working on privacy enforcement, versus the 180 staff of the Irish Data Protection Commissioner). To take a leading role the United States should adopt a GDPR-like standard and establish world-leading enforcement expertise. Cutting edge enforcement of common principles-based standards is *de facto* leadership.

SUPPLEMENTAL POINTS

1. Accountability requires the concepts of "data controller" and "data processor".

Accountability, one of the NTIA's desired outcomes, is difficult to obtain where widespread use of personal data is concerned, and requires that certain data protection concepts be established in law.

First, among these is the concept of a "data controller", which assigns responsibility. This concept is present in the 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, and has been endorsed by the United States.

Second, a federal law should follow the the GDPR model of requiring contracts between controllers and "data processors" who process data on their behalf, in order to establish a paper trail and transparency. A data processor is a company that follows the instructions of a data controller, and takes no role in determining how data are used. A cloud storage service, for example, would normally be a data processor.

Third, it may also be useful to require that data controllers register with a supervisory authority, as is required in the United Kingdom and in other jurisdictions.

2. Notice and consent should not be discounted prematurely.

The NTIA rightly wishes to avoid the prospect that the incomprehensible consent notices that clutter the screens of consumers in the EU would migrate to the United States too. However, the majority of consent notices currently in Europe do not correspond to requirements in the GDPR. Rather, this is "consent theatre", prompted by the tracking-based online advertising industry, which faces particularly grave privacy challenges under the GDPR.

Indeed, these notices are currently the subject of official investigations by privacy regulators across the EU, with the first round of enforcement due in the coming months. Therefore, it will be some time before the GDPR is properly implemented. It would be premature to judge notice and consent by the current state of European consent notices.

CONCLUSION

We at Brave are encouraged that the NTIA has adopted a user-centric view. We commend the Administration's risk-based approach, and its recognition of the need to protect innovation and small and medium sized businesses.

The National Telecommunications and Information Administration has sought contributions to two important questions. First, what are the pillars for a user-centric consumer privacy policy in the United States? Second, what is the ecosystem that provides these pillars?

In response to the first question, we urge the NTIA to consider the merits of a federal law, which draws upon the NTIA's privacy outcomes, and also meets the standard of the the GDPR and Convention 108+.

In response to the second question, we note the "enforcement race" currently underway, and urge the NTIA to consider the need to mandate an increase in enforcement capacity in a federal law, as a means to leverage the emerging GDPR-like standard to build United States leadership.

We further recommend that the NTIA convene a discussion that includes officials from the European Commission and the Council of Europe, and representatives of civil society, and industry to consider these issues. Industry participants should include new market entrants that value the opportunities created by the new GDPR standard, and Brave would be delighted to contribute.

I would also be delighted to do so brief you on the impacts of privacy and privacy law on the online media and advertising industry.

Sincerely,

Dr Johnny Ryan FRHistS
Chief Policy & Industry Relations Officer
Brave