Centre for Information Policy Leadership
Hunton & Williams LLP

30 ST MARY AXE
LONDON EC3A 8EP
TEL +44 (0)20 7220 5700
FAX +44 (0)20 7220 5772

2200 PENNSYLVANIA AVENUE
WASHINGTON, DC 20037
TEL 202 955 1500
FAX 202 778 2201

COMMENTS ON THE FEDERAL COMMUNICATION COMMISSION'S NOTICE OF PROPOSED RULEMAKING ON PROTECTING THE PRIVACY OF CUSTOMERS OF BROADBAND AND OTHER TELECOMMUNICATION SERVICES

WC DOCKET NO. 16-106

SUBMITTED VIA ELECTRONIC FILING

May 20, 2016

The Centre for Information Policy Leadership (CIPL)[1] appreciates the opportunity to respond to the Federal Communication Commission's request for comments on the Notice of Proposed Rulemaking (NPRM) on Protecting the Privacy of Customers of Broadband and Other Telecommunication Services that was released on April 1, 2016. CIPL supports the attention given by the FCC to the issue of privacy protections for the personal information of customers of Internet Service Providers. As a global information and privacy policy think tank, CIPL has been on the forefront of a wide range of policy debates and initiatives around the world relating to improving privacy protections for individuals. One of the core questions that underpins the entirety of our work in this area is how to achieve effective privacy protections in ways that also enable technological innovation and the full range of beneficial data uses made possible by the modern information age. We believe that the FCC's proposal reflects the same concern.

However, in one significant way we believe it may not. Thus, we would like to focus our comments on this particular issue as we have been exploring it in other contexts that, nevertheless, may be relevant and instructive to the context of the NPRM. Specifically, we would like to address the potential over-reliance in the NPRM on the concept of affirmative express consent or "opt-in approval", which we believe is out of step with a trend in forward-looking privacy regimes around the world that recognize the increasing limitations of consent in the modern information age. In that view, overreliance on consent and individual control will likely result in significant impediments to putting personal data to beneficial and productive uses, thereby frustrating or slowing down economic and social advancements without

[1] CIPL for Information Policy Leadership (CIPL) is a privacy and data protection think tank in the law firm of Hunton & Williams LLP and is financially supported by approximately 42 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices to ensure effective privacy protection in the modern information age. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Note that nothing in this submission should be construed as representing the views of any individual CIPL member or of the law firm Hunton & Williams.

countervailing benefits to privacy or to individuals. Below, we highlight a few key considerations on this subject, attaching several of CIPL's more detailed papers on the subject.

Rethinking Consent and Developing Alternative Measures for Privacy Protection

- **The problem with consent**

Privacy policy makers and regulators around the world are grappling with the issue of consent and what role this traditional core privacy principle can and should continue to play in the modern information economy. Many believe that big data, the IoT, and the sheer size and complexity of the digital economy have eclipsed the relevance and usefulness of affirmative, express consent in an increasing number of contexts. Thus, more and more policy makers and regulators are looking for alternatives to consent for use in contexts where consent is no longer practical or effective.

- **Alternatives to consent**

Alternatives to consent already exist. By way of one example, both the EU Data Protection Directive[2] and the new EU General Data Protection Regulation[3] permit data processing on the grounds of "legitimate interest", which allows for data processing in contexts where consent is not feasible and if the processing is necessary for the purposes of the legitimate interests of the business or a third party and these interests are not overridden by the interests or fundamental rights of the data subject. Thus, it essentially allows for processing on the basis of a favorable benefits/risk analysis rather than consent.[4]

This basis for processing is being considered and incorporated into other legal regimes around the world. For example, the two principal Brazilian draft privacy laws making their way through the legislative process in Brazil include "legitimate interest-based" processing. **[Add more examples]**

---

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, No. L 281/31, Art. 7(f).

[3] General Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 6(f), published on 8 April 2016 following the European Council's adoption of its position at the first reading of the Regulation, available at <http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf>. On 14 April 2016, the European Parliament approved the GDPR.

[4] The EU's "legitimate interest" basis for data processing, while useful as an example of the fact that alternatives to consent are important and currently in use, has questionable limitations of its own, such as the fact that it does not apply to processing of "special categories of personal data", including data revealing race, ethnicity, religious beliefs, or data concerning genetics, health and sexual orientation, among other sensitive data. *See* EU GDPR, Article 9. In the accountability and risk-based frameworks we are proposing below and in our attached materials, the sensitivity of the data would be one factor to consider in a benefit/risk analysis and in the selection of appropriate mitigations and controls.

Further, the discussion paper "Consent and Privacy" released by the Canadian Office of the Privacy Commissioner just last week, asks whether Canada should adopt a similar option for processing without consent (among other alternative options). It suggests that Canada may have to rethink its privacy law's current reliance on consent "[g]iven the challenges to the consent model in the digital environment."[5]

CIPL has addressed the challenges of consent and the possible solutions in a number of white papers and articles. Rather than recapping them at length here, we simply attach them for your detailed review.

- **CIPL papers on consent and alternative frameworks of protection**

The first is a short article entitled **"Empowering Individuals Beyond Consent,"** which was first published by the IAPP in July 2015. It describes the ineffectiveness of consent in an increasing number of contexts and points to several alternative measures that can be used to protect and empower the individual in the modern information age. It does not argue that consent can and should not be improved through better transparency and choice mechanisms where consent still is feasible and appropriate. (See Appendix A).

The second is a discussion paper on **"The Role of Enhanced Accountability in Creating a Sustainable Data-Driven Economy and Information Society,"** which we issued in October 2015. It discusses how in contexts where individual control, choice and consent are not practicable or feasible (because, for example, the intended data uses and flows are too complex, manifold, or even yet unknown), the responsibility of privacy protections must fall on the business rather than the consumer. It further describes how this responsibility can be discharged through a number of measures, all of which are encompassed by the concept of "enhanced accountability," which means that an organization has a comprehensive accountability or information management and privacy compliance program in place that includes effective transparency measures, benefit/risk assessment, training, internal oversight, written policies, privacy by design, complaint handling and dispute resolution, as well as frameworks for "fairness" and ethical considerations, all of which would be subject to governmental oversight and enforcement. Within this framework, effective transparency will have the important role of explaining the value-exchange between individuals, society and the organizations that put data to beneficial uses (including unknown future uses) as well as the measures taken to protect individuals from harm, thereby creating public trust that data will be used responsibly. The paper argues that organizations that implement such enhanced accountability frameworks with respect to their information collection and use practices should be able to use information in all ways commensurate with the opportunities of the modern information age even where specific consent is not available or practicable. (See Appendix B)

[5] "Consent and Privacy – A discussion paper exploring potential enhancements to consent under the Personal Information Protection and Electronic Documents Act", Office of the Privacy Commissioner of Canada, May 11, 2016, available at https://www.priv.gc.ca/information/research-recherche/2016/consent_201605_e.asp.

The third is a discussion paper on **"The Role of Risk Management,"** which we issued in February 2016. In that paper, we focus specifically on risk assessment as one of the core elements of any accountability framework. Effective benefit/risk assessments with respect to proposed data uses will enable businesses to understand the potential harmful impacts of their proposed products and services on individuals (taking into account the purpose and scope of the proposed use, the nature of the data, including its degree of sensitivity, among other factors) and enables them to make better decisions about whether and how to proceed with the proposed use and what mitigations and controls to implement in light of the specific risk and benefits. Formalized and structured risk assessments also enable businesses to demonstrate their accountable decision-making processes to enforcement authorities in the event of an investigation. (See Appendix 3)

- **The effects of consent under the NPRM**

We believe that the issues and potential alternatives to consent discussed in these papers are directly relevant to the NPRM's proposal to require opt-in consent for sharing customer PI with certain affiliates and third parties or for using information for the ISP's own unrelated purposes.

The NPRM asks in paragraph 128 whether ISPs and their affiliates "need or benefit" from using customer PI for non-marketing purposes and "what are those uses and are they consistent with consumer expectations?" However, the nature of the modern information economy, including big data, the IoT and other components of this environment, ensures that the question of "what are those uses" cannot always be answered in advance with any specificity.

Indeed, this is precisely the value of modern information uses that must be protected. Analyzing and combining data in new ways may lead to unexpected insights and uses that will be beneficial not just to individual businesses, but also to consumers and society. The Canadian consent report notes that modern technology can result in future uses of data that "defy our imagination" and that are "difficult to anticipate" and thus can't be governed by a "consent" that was given at the time when the data was collected.[6] In many instances, requiring opt-in consent for the entire range of known, possible or yet unknown future beneficial uses of data would not only overwhelm and burden individuals, thereby undermining true individual control and empowerment, it would also likely result in a chronic failure to give consent for no good reason simply because the individual cannot or won't dedicate the time and energy to consider the request. Thus, we believe that any aspect of the NPRM that potentially hinders the beneficial uses of information for new purposes should be subjected to intense further scrutiny and compared to alternatives that are equally or more protective of privacy and the individual,[7] as outlined in our attached papers.

[6] *Id.* At 7

[7] For similar reasons, we would also discourage the FCC from adopting *ex ante* rules limiting the collection of customer data by ISPs. Data collection limitations would interfere with beneficial data uses in similar ways as requiring opt-in consent would and would have negative societal consequences. Any risk to individual privacy can and must be minimized through the alternative means discussed in our papers.

- **The relevance of the FTC model**

We also note that the accountability-based alternatives we propose, including and particularly the benefit/risk assessment element of such accountability-based frameworks, are very much in line with the FTC's privacy enforcement model under its "unfairness and deception" authority. Particularly the unfairness standard, which requires businesses to weigh the countervailing harms and benefits of an action and be able to prove the legitimacy of their analysis to a regulator, provides a framework that is better suited to the modern information context where using information will as a matter of necessity become less and less a matter of individual control and more and more a matter of fair and responsible processing of data, backed up by credible oversight and enforcement.

Thank you for accepting and considering our comments and recommendations. If you have any questions about this submission, please contact Bojana Bellamy, President, Centre for Information Policy Leadership, bbellamy@hunton.com or Markus Heyder, Vice President and Senior Policy Counselor, Centre for Information Policy Leadership, mheyder@hunton.com.