November 6, 2018

Submitted electronically via privacyrfc2018@ntia.doc.gov

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

Re: Docket No. 180821780-8780-01

To Whom it May Concern:

In response to your request for comments, the Agelight Advisory Group and its working group the Online Trust and Integrity Council, have provided the following feedback. As a research and advisory think-tank, Agelight helps the public and private sectors accelerate the adoption of security and privacy-enhancing practices while promoting innovation, ethical privacy practices and the importance of meaningful self-regulation.

We commend NTIA for taking the initiative to help foster the development of a set of user-centric privacy policies and practices, setting high-level goals and best practices for the ecosystem. As GDPR and others nations' regulations and policies have eclipsed those of the US, this is an opportunity for the US to re-gain privacy leadership.

Recent research indicates that over half of internet users surveyed around the world are more concerned about their online privacy than they were a year ago, reflecting growing concern around the world about online privacy.[1] Now is the time to establish a consistent regulatory framework that is extensible to new technologies and applicable to all industry sectors.

With the increase reliance of connected devices in our homes and society at-large, the collection, use and sharing our digital life styles are increasingly at risk. The aggregate impact and the lack of regulations has raised significant long-term risks to consumers and businesses alike. Combined with the mounting privacy implications of facial recognition, advances in artificial intelligence (AI), device fingerprinting and use of biometrics, any such privacy framework must be agile and extendable to these and other evolving technologies. Internationally the call for guiding principles to preserve human rights in the development of artificial intelligence is growing citing the potential risks induced by the current trend of market concentration.[2] Not only will consumers benefit from such a framework and "privacy

[1] 2018 CIGI-Ipsos Global Survey on Internet Security and Trust https://www.cigionline.org/internet-survey-2018

[2] International Conference of Data Protection and Privacy Commissioners declaration https://icdppc.org/wp-content/uploads/2018/10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf

guardrails", but industry will as well, through removing the uncertainty of the legal environment and ability to innovate and promote economic growth.

As outlined by the RFC, users need to have fundamental privacy rights including clear disclosures, transparency and controls on the collection use and sharing of their data. We concur with industry leaders including Microsoft and Apple, recognizing privacy is a "basic human right" and the need to embrace ethical data privacy practices.[3]

To this point we agree with NTIA on the need to shift from the lengthy and at times convoluted privacy notices. As advocated by leading researchers, consumer advocates as well as many within the FTC for the past decade, now is the time to embrace a standardize short format, not unlike food nutrition labels or a Monroney car sticker established over 60 years ago.[4,5] Such efforts will help enable consumers to make informed, fair and educated choices regarding their personal and sensitive data. A secondary benefit includes the ability for a user to make comparisons on a product and service, not unlike comparing product warranties, the nutrition content of the food they eat or the performance of an automobile they may purchase.

While it is acknowledged the United States has a history of providing strong privacy protections, the US has fallen behind the rest of the world. When considering high-level goals, the US needs to consider incorporating many of the practices put forth in the GDPR and established by other countries including Canada, Australia and others. As the internet transcends geographic boundaries, such a framework must be in lockstep and alignment with the rest of the world. The recent draft legislation put forth from Senator Wyden is a significant step towards many of the goals outlined in the RFC.[6]

Today the Federal Trade Commission, (FTC), is limited to protect consumers' privacy due to a combination of limited resources, lack of the rule-making capabilities and limited enforcement abilities. Reliance on enforcement of Section 5 of the FTC Act regarding unfair and deceptive business practices, has had limited impact to the harms and abuses taking place today.

In the absence of any Federal data breach, privacy or security baseline requirements, businesses have been burdened with a patchwork of state laws which are cumbersome and hinder innovation. Ideally robust Federal legislation would pre-empt State laws, with the provision for State right of enforcement, modeled under similar provisions provided under the CAN-SPAM Act of 2013.[7] Any federal framework needs to be interoperable with other legal structures worldwide, protect digital innovation and put the owners of data first rather than those who profit from it.

NTIA is to be commended for its efforts to convene multi-stakeholder efforts and this continued leadership is needed. At the same time, we need to learn what has worked and where there is room for improvement. Two positive examples under NTIA's leadership include IoT patching and updates and

[3] https://www.cnbc.com/2018/11/01/microsoft-ceo-tech-companies-need-to-defend-privacy-as-a-human-right.html

[4] Privacy Labels https://cups.cs.cmu.edu/soups/2009/proceedings/a4-kelley.pdf

[5] The Automobile Information Disclosure Act of 1958 https://www.gpo.gov/fdsys/pkg/USCODE-2010-title15/html/USCODE-2010-title15-chap28.htm

[6] Consumer Data Protection Act – Discussion Draft https://www.wyden.senate.gov/imo/media/doc/Wyden%20Privacy%20Bill%20Discussion%20Draft%20Nov%201.pdf

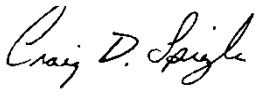
[7] Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act). https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/can-spam-rule

vulnerability disclosures working groups.[8,9] Unfortunately past privacy centric efforts have been less than successful and unable to archive stakeholder consensus. Examples include the mobile privacy disclosures and the facial recognition working groups.[10,11] Much can be learned from these efforts including the need to structure working groups so they are not dominated by the self-interests of trade groups and their lobbyists.

In summary, US citizens and businesses need to have the same or possibly enhanced rights as other developed nations. We agree with many of the goals outlined in the RFC including considering the impact on small businesses; making the framework technology neutral while minimizing compliance costs. Simply put consumers need to have the ability to opt-in and know what is being collected, used and shared. Agelight advocates any privacy framework embrace the following goals:

- Be extensible and flexibly to accommodate evolving and emerging technologies and definitions of personal and sensitive information;
- Comprehensive application and a level playing field across all sectors and industries;
- Interoperability to allow data to move seamlessly across borders, (i.e. Privacy Shield);
- Develop incentives for organizations who embrace security and data protection best practices and norms;
- Provide the FTC resources including rule making and enforcement authority and
- Integrate metrics to track industry adoption including the benefits and impact of any such framework including self-regulatory efforts.

We look forward to working with the Administration to develop a framework as outlined above, harmonizing global interoperability, promoting ethical data privacy practices while prioritizing meaningful privacy and security for consumers.



Craig D. Spiezle
Managing Director, AgeLight Advisory Group
https://agelight.com

[8] Multi-stakeholder Process; Internet of Things (IoT) Security Upgradability and Patching https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security

[9] Multi-stakeholder Process: Cybersecurity Vulnerabilities https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities

[10] PC World - A federal push for mobile privacy has failed, critics say https://www.pcworld.com/article/2047775/critic-ntias-mobile-privacy-push-has-failed.html

[11] https://bits.blogs.nytimes.com/2015/06/16/consumer-groups-back-out-of-federal-talks-on-face-recognition/ & https://www.eff.org/deeplinks/2015/06/eff-and-eight-other-privacy-organizations-back-out-ntia-face-recognition-multi