In the Matter of

Federal Communications Commission’s Request
for Comments on the Notice of “Protecting the Privacy of Customers of Broadband and Other Telecommunications Services”

WC Docket No. 16-106

COMMENTS OF

THE INFORMATION ACCOUNTABILITY FOUNDATION

The Information Accountability Foundation (“IAF”) wishes to thank the Federal Communications Commission for the opportunity to comment on its proposed broadband privacy rulemaking. The IAF is a 501(c)(3) non-profit research and educational foundation whose mission is forward-looking, balanced information policy. The word “accountability” in our name gives a sense of our approach to information policy. The IAF is the 2013 incorporation of the Global Accountability Dialogue, a multi-stakeholder process involving regulators, business, and civil society that developed and socialized the “Essential Elements of Accountability.”¹ The Essential Elements have since been incorporated in privacy law and practice in Europe, Asia, and North and South America. It is from the perspective of accountability that the IAF will approach the FCC rulemaking.

These comments reflect the views of staff and do not necessarily reflect the views of IAF’s board of trustees or funders.

Introduction

The FCC proposed rulemaking suggests three foundational elements of privacy: transparency, choice, and security. These elements are the building blocks for U.S. Internet privacy as it has emerged since the first web browser in 1993. The foundational elements place the onus on individuals to read privacy notices and make a choice – typically, the ability to say “no” to a collection and onward use of data and to say “yes” to other sensitive uses of data. They also reflect a partial set of the OECD Guidelines adopted in 1980 and revised in 2013. They only reflect half of the interests captured by privacy and data protection law.

Privacy law has always been designed to protect personal freedom and to allow information to be used with confidence. So, privacy laws, since their first inception in the early 1970s, have attempted to balance both personal and societal interests, choice by individuals and fairness requirements on organizations that are the stewards of the information and create value through the use of information. To achieve these ends, privacy law has had two facets. The first is personal control to enable individual autonomy. Autonomy is exercised through a specification by the organization of what data will be collected and how it will be used and the opportunity of the individual to say “use” or “not use” to that collection and use of data. This functionality is captured in the proposed rulemaking as transparency and choice.

The second facet is accountability by requiring organizations to put in place mechanisms to fairly process data, over and above choice, in a fashion that is safe and balanced. The security requirement in the proposed rulemaking is responsive to fair processing but does not reflect all aspects of fair processing. Fair processing also requires organizations to understand the risk they create for others, the benefits created by processing, how the risks are mitigated, and how the benefits are judged in light of the related residual risks. This is often referred to as privacy by design. Much of the work on accountability has been refined based on collaboration between business, enforcement agencies, academics, and advocacy organizations.

Privacy law is not just about controls. A clear objective of the law is creating a playing field where data may flow to its best use. This often requires an assessment of the risks associated with data processing, the benefits that come from the processing, who bears the risk, and who gets the benefits. The term proportionality is often used in conducting a privacy analysis. Are the benefits to individuals and society proportional to the economic and societal value that comes from the processing?

Privacy and data protection law and the business procedures associated with the processing of data in a legal, fair, and just manner are undergoing revision to catch-up with the massive changes taking place in information and communications technologies. The European Union’s General Data Protection Regulation (“GDPR”) is just the first wave of those modifications. Changes will also be seen in Latin America, Canada, Asia, and Africa. Some changes will be explicit in revisions of laws, while other changes will use the flexibility built into laws (e.g., codes of conduct) to align interests of all stakeholders.

Change does not mean the abandonment of key societal values captured by privacy law. Those values include the link between privacy and democratic political systems, the right to be free of digital predestination, and fair processing that aligns the various interests of all stakeholders but with a special emphasis on individuals’ various interests. At the same time, fair processing should enable data to create knowledge-based value. The development and implementation of new governance concepts requires a full, 360-degree view of the dynamics in play. Information policy cannot be dependent on a single approach.

The balance between autonomy and fair processing has changed significantly since the early 1970s. Back in 1970, almost all data was collected directly from an individual in a manner where the individual was aware of that collection. Notices were merely a reflection of very simple transactions. Fast forward to 2016 where the smartphone is the hub for a very complex ecosystem. In 2013, the Global Accountability Dialogue conducted a session in Warsaw where we identified six different classes of
parties that were collecting data from the individual’s handset. Today, when one adds wearables and beacons, the number of user classes is substantially larger. A privacy notice that truly would reflect the complexity of this ecosystem would probably be 45-pages long or longer and would not be overly useful in informing a choice.

The changing nature of data is increasingly being recognized worldwide. On May 12, 2016, the Office of the Privacy Commissioner of Canada issued “Consent and Privacy: A discussion paper exploring potential enhancements to consent under the Personal Information Protection and Electronic Documents Act.”

Consent is the term most often used in privacy law outside the United States. The paper argues that the limits of consent, even under a law that is highly consent based, must be revisited because of the changes in technology since the year 2000.

Canada is not alone. The European Union’s new privacy legislation, the GDPR, was enacted in 2016. That legislation recognizes both privacy facets. The law does not rely only on consent to legitimize processing. There are five other means for establishing processing is appropriate. The law also suggests that consent should be used when it is the suitable permission, but other legal basis should be used when they are more appropriate. While the IAF would not endorse the prescriptiveness of the new European law, we believe the more nuanced approach to permitting data processing is laudable.

IAF Concerns from an Accountability Standpoint

The FCC proposes rulemaking in 2016 based primarily on the first privacy facet, autonomy. IAF staff feels that privacy rulemaking should be based on both privacy facets and believes there is a cost associated with only looking at autonomy. We would recommend the rulemaking include the objectives of an accountability-based privacy program without being overly prescriptive on organizations as to how they should meet these objectives.

The IAF staff believes that individuals should have control over data collection, aggregation, creation, and use where they can effectively do so. Has the FCC asked itself whether open networks, with numerous responsible parties, are the medium in which individual control is the most effective means for governance?

Today’s processing, in many cases, cannot be simply described. Therefore, a decision to allow processing based on either an incomplete but simple notice, or a complete but hardly understandable notice, does not lead to effective governance. Rather than forcing opt-in controls that preclude future uses that may well meet individual or societal needs, would an accountability-based system that includes risk assessments with integrity not be preferable?

The IAF believes transparency is more important than ever, but transparency is not a notice to inform choice. IAF, in forthcoming work on Effective Data Protection Governance, will describe a complete notice whose audience is regulators and lawyers but would be available to consumers as well. Will the types of purpose specification notice the FCC is suggesting truly inform individuals in an effective manner? If not, why would it not be more effective to encourage experimentation on means to truly

---

inform people about how data that pertains to them might be used? IAF suggests that transparency should include other elements that assist individuals in understanding how data is used but does not force them to be data’s governor. Would it not make sense for the FCC to ask similar questions about transparency, such as the ones that are being posed in Canada?

Advanced analytics, often referred to as big data, is increasingly driving innovation. While big data in advertising is most visible, big data also drives innovation in cyber security, product development, education, and individualized medicine. Big data may be separated into “thinking with data” and “acting with data.” This concept was first articulated in “Big Data Analytics: Seeking a Foundation for Effective Privacy Guidance.”\(^3\) Thinking with data is where new insights are developed and is most often a repurposing of data. This data use must be governed to protect individuals; however, consumer choice is not the most effective means for governance. Instead, accountability becomes appropriate. The IAF’s “Unified Ethical Frame for Big Data Analysis”\(^4\) describes an accountability-based governance process that might be applied when thinking with data. How that process might be overseen was further developed in “Enforcing Big Data Assessment Processes.”\(^5\)

The IAF’s primary concern is that the nature of transparency and choice mandated by the new rules would preclude thinking with data, resulting in lost innovation and higher costs on individuals, business, and society as a whole. Furthermore, as mentioned earlier, there are many essential key players in today’s and tomorrow’s information ecosystem. It seems to us that the proposed rulemaking that impacts one player creates a very awkward governance system and that awkwardness overshadows the entire ecosystem.

We would reiterate that the IAF is not opposed to individuals having control over their data where the risks of data collection and use are truly disproportionate to the value being created for individuals and society. In fact, we would endorse such controls. However, that would require a sense of proportionality that does not seem to be part of this rulemaking.

Finally, it is key the FCC rulemaking be in line with and interoperable with other International laws and market expectations. When other legal systems are looking beyond notice and choice, does it make sense for the FCC to create a rule that is less flexible than systems that are evolving in other parts of the world.

The fact is that broadband technologies will be the conduit for much of the data that will be used when thinking with data. IAF staff believes that the three foundational elements described in the rulemaking are not the best approach for enabling individual interests that are much broader than just autonomy. We believe FCC staff should look at the work that has been conducted on data stewardship over the


past six years and consider how accountability might be encouraged to both enable the protection of individuals and to benefit all the stakeholders from thinking with data.

Thank you again for the opportunity to comment.

Respectfully Submitted,

Martin Abrams  
Peter Cullen  
Lynn Goldstein  
Nick Warren  
The Information Accountability Foundation  
A Non-Profit Charitable 501(c)(3) Organization  
Tax ID: #46-1416947  
1811 River Heights Dr.  
Little Rock, AR 72202  
(972) 781-6667

Date: 5/24/2016