Before the

NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION

U.S. DEPARTMENT OF COMMERCE

Washington, DC

In the Matter of	)	
A Multistakeholder Process To Develop	)	Docket No. 120214135–2135–01
Consumer Privacy Codes of Conduct	)	
	)	

COMMENTS OF

THE INFORMATION TECHNOLOGY AND INNOVATION FOUNDATION

April 2, 2012

Daniel Castro

Information Technology and Innovation Foundation[1]
1101 K Street NW, Suite 610
Washington, DC 20005

[1] ITIF is a nonprofit, non-partisan public policy think tank committed to articulating and advancing a pro-productivity, pro-innovation and pro-technology public policy agenda internationally, in Washington and in the states. Through its research, policy proposals, and commentary, ITIF is working to advance and support public policies that boost innovation, e-transformation and productivity.

Introduction

The Information Technology and Innovation Foundation (ITIF) is pleased to submit these comments in response to the National Telecommunications and Information Administration's (NTIA) request for comment on the "multistakeholder process to develop consumer data privacy codes of conduct." Primarily these comments will address NTIA's inquiry into what issues should be addressed through the privacy multistakeholder process and how stakeholder discussions of the proposed issues should be structured to ensure openness, transparency, and consensus building.

Consumer Data Privacy Issues to Address Through Enforceable Codes of Conduct

NTIA has stated its intent to initiate a multistakeholder process to address different privacy issues. The government has an important role to play as a facilitator and convener to encourage the development of technologies that have economic benefits or improve quality of life. Certainly there are many technologies under development that could benefit from more discussion and debate about how to properly integrate consumer privacy protections. These include privacy issues relating to mobile devices, electronic identification, mobile payment systems, sensor networks, cloud computing, and biometrics, among others.[i]

While some of these technologies involve complex privacy issues, many uses of these technologies do not represent any threat to consumer privacy. Furthermore, many uses of these uses of consumer data may be in line with commonly accepted practices. To facilitate the unimpeded development of these technologies, it would be useful to create a precise and robust model for determining when a certain use of data falls under this category of "commonly accepted practice." Developing such a model would be a good area for a multi-stakeholder task force to explore more thoroughly.

Two important considerations for determining whether an issue should be taken up in the consumer privacy multistakeholder process are 1) the degree to which consumers are facing harm or potential harm; and 2) the degree to which existing self-regulatory efforts are already underway.[ii]

NTIA should not engage in consumer privacy rulemaking simply as an end in itself. Instead, NTIA should choose areas for a multistakeholder process where there is convincing evidence that consumers are being harmed or may face a reasonable expectation of harm in the future. This means that NTIA should develop expertise in identifying the types of harms that consumers face from violations of their privacy and what countermeasures appropriately safeguard against these potential harms. The NTIA should not initiate this process for potential privacy harms that are purely speculative or that consumers do not have a high likelihood of facing.

NTIA should also choose issues for the multistakeholder process where there are inadequate or non-existent self-regulatory efforts underway, not just those areas where some privacy advocates may feel self-regulatory efforts have not moved fast enough or include the appropriate rules. NTIA should not create new parallel efforts where existing industry self-regulation already exists as this may discourage participation in current industry-led self-regulatory efforts. Similarly, creating redundant efforts could encourage participants in self-regulatory efforts to "re-litigate" any points that they may have lost in the self-regulatory arena and generally result in a less efficient rulemaking process.

Finally, NTIA should recognize that a government-sponsored multistakeholder approach may not always be the best solution to a given privacy challenge. For example, some privacy challenges may be better addressed by creating new rights or protections for consumers rather than creating new rules on how businesses manage data. At times other solutions, ranging from government oversight to legislation, may be more appropriate.

Implementing the Multistakeholder Process

Creating a multistakeholder process for addressing challenges on the Internet can help ensure that different perspectives are represented rather than the narrow interests of a few companies. This is one reason why consent agreements between companies and the Federal Trade Commission (FTC) should not be used as the basis for industry-wide privacy regulations. These consent agreements are created outside of a multistakeholder process and may not properly represent all interests. However, a multistakeholder process does not guarantee that all sides of an issue will be represented equally or fairly. Therefore it is important for NTIA to ensure that the multistakeholder process does not become a forum for anti-competitive activity. This is particularly true for industries where stricter privacy regulations might "grandfather in" current businesses and serve as a barrier to entry for new competitors. For example, in a recent report Lundblad and Masiello demonstrate how opt-in requirements for consumer information encourage providers to broaden the scope of data they ask for, desensitize users to making decisions about sharing personal data, and raise the switching costs leading to less competition and lock-in.[iii] It is clear that privacy rules and regulations could be used to protect the interests of certain stakeholders. Alternatively, other rules that may encourage competition, such as data portability, may be overlooked.

Similarly, it is important that the multistakeholder process does not prohibit future innovations or business practices that are not represented by the current set of stakeholders. For example, some companies today might agree to a data minimization principle because they already have a working business model, product or service that does not depend on more data. However, a start-up company a few years from now might find this type of rule unnecessary and too restrictive. For example, a data minimization rule may discourage businesses from collecting data unless they have pre-defined plans for how they will use for this information. This requirement would limit the ability of businesses to conduct post-hoc analysis to develop new types of products and

services based on what they learn from the data, even if these organizations use this data in a way that protects individual privacy. It is important for the multistakeholder process to recognize that there will be many voices not represented and take steps to protect these interests as well. The NTIA should consider how to protect these interests because consumers will benefit from future innovations, not just current innovations.

It is also important to consider the framing of the questions NTIA looks at in the multistakeholder process. For example, NTIA advised that it is considering focusing on privacy notices for mobile apps for the initial multistakeholder process. While it correctly highlights the importance of transparency for consumer privacy, NTIA should not begin the multistakeholder process with a preconceived objective, such as to create a set of simple mobile privacy notices. For example, in this case, privacy policies may be complex because they involve a complex set of data, business practices, privacy protections, and relationships. Requiring companies to pigeonhole themselves into a set of predefined, one-size-fits-all businesses practices does not foster innovation.

A better approach would be for NTIA to identify a consumer privacy harm that it can address. This should get to the core issue at stake, rather than a superficial manifestation of the issue. For example, in this case, a problem statement could address the underlying potential for consumer harm from downloading an untrustworthy app. Solutions to a problem look very different depending on the problem statement. For example, the solution to the problem "how might we simplify consumer privacy notices?" is likely very different than to the problem "how might we protect consumer information in mobile apps?" If we use the former, alternatives solutions, such as third-party certification or technical standards for apps or mobile operating systems, may be overlooked. NTIA should have an open and collaborative process to develop these types of questions. NTIA should also look to use innovative online platforms to better engage with a diverse set of stakeholders and ensure transparency throughout the multistakeholder process.[iv]

In all of these discussions, stakeholders should recognize that privacy is but one of many values that consumers hold, and protecting privacy should be balanced against other competing interests. The objective of the process should not be to maximize privacy regardless of cost, but rather to find the right balance between different goals and objectives.

Conclusion

The end result of a multistakeholder process on consumer provider should not be merely to achieve consensus, but to develop a rich understanding of the tradeoffs between different proposed rules. This will require not only developing an understanding of current business practices, but also considering how these rules might impact future practices. In constructing these set of rules, policymakers should remember that protecting privacy is not the same thing as protecting consumers. Consumers benefit from many protections, including ensuring that their

data is not misused and that competitive markets produce more innovation, choice and efficiency.

Endnotes

[i] ITIF has written extensively about all of these topics. See for example, Daniel Castro, "Explaining International Leadership: Electronic Identification Systems," Information Technology and Innovation Foundation, September 2011, http://www.itif.org/files/2011-e-id-report.pdf, Daniel Castro, "No Longer a Nameless Face in the Crowd," ITIF, June 10, 2011, http://www.itif.org/publications/no-longer-nameless-face-crowd, and Daniel Castro, "Cloud Computing Requires National Policy Leadership," ITIF, August 2010, http://www.itif.org/files/2010-cloud-computing.pdf.

[ii] For a detailed look at self-regulation and online privacy, see Daniel Castro, "Benefits and Limitations of Industry Self-Regulation for Online Behavioral Advertising," Information Technology and Innovation Foundation, December 2011, http://www.itif.org/files/2011-self-regulation-online-behavioral-advertising.pdf.

[iii] Nicklas Lundblad and Betsy Masiello, "Opt-in Dystopias," SCRIPTed 7, no. 155 (2010), http://www.law.ed.ac.uk/ahrc/script-ed/vol7-1/lundblad.asp.

[iv] For example, the Consumer Financial Protection Bureau used online engagement to better design financial disclosure documents with its innovative "Know Before You Owe" effort. For details, see http://www.consumerfinance.gov/knowbeforeyouowe/.