UT LAW CLE THE UNIVERSITY OF TEXAS SCHOOL OF LAW

PRESENTED AT

29th Annual Technology Law Conference

May 26-27, 2016
Austin, Texas

Comments on the FCC's Notice of Proposed Rulemaking "Protecting the Privacy of Customers of Broadband and Other Telecommunications Services" Submitted by The Information Accountability Foundation

Martin Abrams

Comments on the FCC's Notice of Proposed Rulemaking
"Protecting the Privacy of Customers of Broadband and Other Telecommunications Services"
Submitted by 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 (WC Docket No. 16-106). 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

[1] The Centre for Information Policy Leadership (CIPL) (2009), "Data Protection Accountability: The Essential Elements", http://www.huntonfiles.com/files/webupload/cipl_galway_accountability_paper.pdf.