



THE FREE STATE FOUNDATION

A Free Market Think Tank for Maryland.....Because Ideas Matter

Perspectives from FSF Scholars

April 5, 2012

Vol. 7, No. 9

Any New Privacy Regime Should Mean An End To FCC Privacy Powers

by

Randolph J. May * and Seth L. Cooper **

On February 23, the White House released its anticipated framework for protecting digital privacy entitled, ["Consumer Data Privacy in a Networked World: A Framework for Promoting Privacy and Promoting Innovation in the Global Digital Economy."](#) The White Paper explaining the proposed framework raises a host of important public policy issues. One significant issue is this: Given the framework's plan to place data privacy enforcement with the Federal Trade Commission, what should become of the FCC's jurisdiction over consumer privacy?

If the White House's framework were to be implemented, FTC jurisdiction over digital privacy should replace the FCC's piecemeal legacy jurisdiction regulating privacy in different ways for telephone, cable, and direct broadcast satellite (DBS) subscribers. Currently, the FCC has regulatory authority over telephone subscriber privacy under Section 222 of the Communications Act and over cable subscriber privacy under Section 551. The FCC also has authority over DBS subscriber privacy under Section 338 of the Satellite Home Viewing Improvement Act.

In today's digital and IP-based converging market, all communications and information services providers and media companies that collect and use personal data should be governed, so far as is practicable and sensible, by a set of common rules under a common enforcer. Without trying to define here the parameters of what should be the

FTC's jurisdiction under any new privacy regime, and without here addressing any proposed expansion of its jurisdiction, transferring data privacy jurisdiction from the FCC to the FTC with respect to communications and media services would give consumers a simpler and more consistent set of privacy expectations. And consolidating such jurisdiction in the FTC would also reduce the likelihood that particular types of information collectors and purveyors would be disadvantaged without justification as a result of their being subject to different privacy regulatory regimes.

The White House's proposed digital privacy framework includes seven general principles to guide expectations for consumer protections in the digital economy. The framework calls for legislation to give the FTC power to enforce those principles and for a multi-stakeholder process to take steps to voluntarily implement the principles through the establishment of codes of conduct that embody a "Consumer Bill of Rights." Service providers who agree to abide by the codes – and who actually abide by them in practice – would gain safe harbor from direct FTC enforcement of the principles. Under Section 5 of the FTC Act, the FTC would adjudicate all disputes on a case-by-case basis.

While the White Paper stops short of endorsing the wholesale replacement of various existing privacy laws, with regard to communications and media companies, the paper recommends the consolidation of privacy oversight in the FTC. The paper explains:

Because existing Federal laws treat similar technologies within the communications sector differently, the Administration supports simplifying and clarifying the legal landscape and making the FTC responsible for enforcing the Consumer Privacy Bill of Rights against communications providers. [Page 39.]

By way of explanation, the paper explains in footnote 49 that Sections 222, 338, and 551 of the Communications Act require "telecommunications carriers, satellite carriers, and cable services, respectively, to protect customers' personal information."

This call for "simplifying and clarifying" the law and for giving the FTC authority regarding communications providers represents a positive development. It acknowledges the fact that provisions that may have been sensible when adopted, such as the privacy protection provisions in the Communications Act, may be rendered much less so – even obsolete – when considered in the context of markets that have changed radically as a result of technological developments and consumer demands.

In today's digital broadband environment, the lines distinguishing different products, services, and provider roles are no longer distinct. Voice, video, and data services are now offered by traditional telephone and cable providers. Competing DBS providers typically offer stand-alone video services or bundled packages that include voice and Internet services through agency resale agreements. Wireless providers also offer voice and data services, with 3G and 4G upgrades now offering downloadable and streaming HD video content. And Internet service provider competitors offer voice applications, video content, and data services over digital broadband facilities through individual

purchases or subscriptions. Meanwhile, at every layer of the Internet, reaching from the core to the edge and throughout, myriad business partnerships and arrangements prevail between companies that are sometimes market competitors and sometimes collaborators. These shifting partnerships and arrangements facilitate today's digital commerce and market transactions. And the labels that formerly applied to the firms at the center of this digital commerce – "telephone," "cable," and "information" companies – borne out of now-outmoded regulatory distinctions, bear little relationship to the establishment of sensible public policy.

Today's technological and marketplace convergence calls for a set of common principles to be applicable for all providers of digital communications and information services that collect and use personal data. From an end-user perspective, simple and consistent rules concerning the privacy of their personal data are most consumer-friendly.

Consistency is also what consumers in converging markets increasingly are going to expect. There is no basis to presume consumers want different sets of basic data privacy protections that depend upon whether they are doing business with, say, a broadband service provider or an online content company. Of course, in many instances a broadband service provider is also a content provider, and vice versa. Nor is there any basis in thinking consumers want different sets of data privacy protections from a single provider depending on the particular service being used at one time or another.

Assuming government oversight, a common enforcer of digital privacy principles and codes of conduct is also important because regulatory policy is often – if not invariably – impacted by the particular regulatory agency charged with its enforcement. Discretionary decision-making upon which enforcement necessarily depends is influenced by an agency's institutional preferences, historic concerns, capabilities, and expertise. Consistency in data privacy policy could be undermined if different agencies – in this instance, the FCC and the FTC – with different priorities and different personnel are given overlapping enforcement and oversight authority.

Disparate privacy regulations for voice and video providers make less and less sense as the Internet ecosystem continues to develop. Therefore, the White House's digital privacy framework appropriately recognizes that the current FCC privacy jurisdiction over telecommunications, cable, and satellite firms should be transferred to the FTC. Assuming the adoption of some new, common-sense privacy regime that properly weighs the costs and benefits of applicable regulatory requirements, authority for consumer digital privacy enforcement should be transferred from the FCC to the FTC. At the very least, providers should be given the ability to voluntarily opt-out from Sections 222, 551, or 338, respectively, upon choosing to comply with any new privacy regime subject to FTC's enforcement jurisdiction.

Reliance on a common set of rules and a common enforcer should be hallmarks of consumer data privacy policy for the 21st Century. Assuming that upon the completion of a thorough vetting and consultative process the White Paper proposal were to result

in the development of a proper regime that is not overly prescriptive or costly, all privacy protection authority that currently resides in the FCC should be transferred to the FTC.

* Randolph J. May is President of the Free State Foundation, a non-partisan Section 501(c)(3) free market-oriented think tank located in Rockville, Maryland.

** Seth L. Cooper is a Research Fellow of the Free State Foundation.