Perspectives from FSF Scholars
October 26, 2012
Vol. 7, No. 31

Vindicating A Voluntary Process For Protecting Digital Privacy

by

Seth L. Cooper *

On October 11, the Government Accountability Office (GAO) issued a report titled "Mobile Device Location Data: Additional Federal Actions Could Help Protect Consumer Privacy." The report briefly described how different segments and providers in the wireless industry collect and use location-based data as well as how they protect consumer privacy. It also looked at ongoing federal agency actions regarding consumer data privacy.

The GAO report recommended that the National Telecommunications Information Administration (NTIA) impose specific timetables for imposing new privacy mandates. It likewise recommended that the Federal Trade Commission (FTC) impose a set of specific guidelines for mobile providers regarding location-based data privacy protections.

But the GAO's recommendations for a more immediate and aggressive federal agency approach to mobile location data privacy are premature at best. At worst, such an approach could derail current efforts to reach consensus about how best to promote consumer privacy consistent with overall consumer welfare. NTIA and the FTC were right to defend the ongoing process for collaboratively establishing standards for protecting consumers' digital privacy.

The NTIA-facilitated multi-stakeholder process holds out the promise for a voluntary, consensus-driven set of common standards for protecting the digital privacy of consumers. Such an approach is better suited to weighing and reconciling intricacies and potential conflicts among consent, choice, access, usability, innovation, and security imperatives than is an approach based on agency dictates. The multi-stakeholder process is in its early stages and proceeding in a reasonably timely manner. It should be given a chance to succeed. The process should not be second-guessed or short-circuited by more rigid agency procedures or premature policy declarations.

In February, the White House released its policy framework for protecting consumers' digital privacy. It includes a so-called "Consumer Privacy Bill of Rights" comprised of seven principles to guide consumer privacy protections in the digital economy. The framework also establishes a multi-stakeholder process for voluntarily implementing those principles through detailed codes of conduct. A series of focused meetings, led by NTIA, are now in the works for achieving consensus on those codes. Digital service providers who agree to follow the codes – and who actually follow them in practice – would gain a safe harbor from direct FTC enforcement of the principles. Under Section 5 of the FTC Act, the FTC would adjudicate all disputes arising under the codes on a case-by-case basis. (This framework was outlined in closing remarks by Daniel Weitzner, then Deputy Chief Technology Officer for Internet Policy, The White House Office of Science and Technology Policy, at FSF's Fourth Annual Telecom Policy Conference.)

The GAO report, as indicated above, zeroes in on a particular aspect of digital privacy, namely: mobile location-based data. As the report explains:

> Smartphones allow users access to location-based services that can provide them with navigation tools and information relevant to their surroundings based on increasingly precise information about the user's current location determined by Global Positioning System (GPS) and other methods…In providing such services, smartphones and the companies that support their functions are able to collect and retain precise data about users' locations.

The GAO report sketches out the benefits of location-based services along with some of the potential risks posed when such services are unaccompanied by privacy protections:

> For the companies, the main purposes for using and sharing location data are to provide and improve services, to increase advertising revenue, and to comply with legal requirements. Consumers, in turn, can benefit from these new and improved services and from targeted location-based advertising. Nonetheless, allowing companies to access location data exposes consumers to privacy risks, including disclosing data to unknown third parties for unspecified uses, consumer tracking, identity theft, threats to

personal safety, and surveillance.

NTIA's response to the GOA (contained in report Appendix II), acknowledged the privacy dynamics relating to location-based services. But it defended the multi-stakeholder approach, pointing to its "history of success in addressing Internet-related issues." The agency reiterated that the initial focus of the multi-stakeholder is on mobile application transparency. According to NTIA, "it appears likely that the stakeholder group will address the transparency of location services in the mobile app context," and also suggests that "mobile location (beyond transparency) is certainly one of the topics under consideration" for discussion as the multi-stakeholder process proceeds.

Results of this focus on mobile app transparency will hopefully provide an indicator of the multi-stakeholder process's overall prospects for success. And before those results come in, calls for new strictures on that process are premature.

As a matter of public administration, there's much to be said for performance goals and timetables for taking action and measuring agency progress. Those kinds of measures are particularly fitting when it comes to an agency's internal control of operations. However, such measures are less fitting for a collaborative effort with outside entitles – such as digital providers and non-profit organizations – involving development of marketplace business practices and consumer expectations regarding complex and rapidly changing technologies, including mobile location-based data services.

Moreover, any near-future FTC guidelines for location-based data services amounts to an agency-driven approach that is quite different from the consensus-driven approach. Adopting such guidelines before the multi-stakeholder process has a chance to run its course could hamper or derail consensus-building efforts.

Once the multi-stakeholder process is concluded and codes of conduct, or "best practices," are in place, a set of FTC guidelines for location-based digital services might make sense. To the extent FTC jurisdiction permits, guidelines based on the "Consumer Privacy Bill of Rights" principles could conceivably be established, with particular regard to the practices of providers who choose not to comply with the codes and obtain safe harbor. However, for any guidance in this area we should first look to the multi-stakeholder process that's now in the works.

While the White House's data privacy framework is directed to commercial use of personal data, the GAO's report does raise concerns about law enforcement access to mobile location-based data. But any necessary actions to address those concerns pose no obstacles to the multi-stakeholder process or prospective codes of conduct. Congress and state legislatures shouldn't hesitate to strengthen or otherwise streamline requirements that law enforcement must meet before obtaining mobile location-based data.

If successful, the multi-stakeholder process should lead to a streamlined common set of standards for all providers of digital services as FSF President Randolph May and I

advocated in a prior *Perspectives from FSF Scholars* essay, "Any New Privacy Regime Should Mean An End To FCC Privacy Powers." The White House's digital privacy framework recognizes that 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 subscribers.

Consumers of digital services are best served by simple and consistent rules concerning the privacy of their personal data, including mobile location-based data. But generating a workable set of rules that accounts for the intricacies and constraints presented by dynamic digital technologies and services will be more likely achieved through collaboration, not agency mandates. The multi-stakeholder process for developing voluntary codes of conduct on data privacy practices offers just such a collaborative approach. That process should be given the space it needs to achieve its purpose.

* Seth L. Cooper is a Research Fellow of the Free State Foundation, a nonpartisan Section 501(c)(3) free market-oriented think tank located in Rockville, Maryland.