

Privacy and Information Governance

Mobile Privacy Landscape Shifts Again: Three New Codes Suggest Three Consensus Points and Three Themes for Consideration

By Mary Ellen Callahan, Michael T. Borgia, David M. Didion and Sabrina N. Guenther

The following is the Executive Summary, for the full analysis of the three codes and how they will impact mobile privacy, please [click here](#).

Three New Voluntary Codes from Government and Industry

Three major voluntary mobile codes were released or hit important milestones last week, adding to the patchwork landscape of recent mobile privacy initiatives:

1. The draft voluntary code of conduct developed during the Department of Commerce's National Telecommunications and Information Administration's (NTIA) multi-stakeholder process will now enter a voluntary testing phase;
2. The Digital Advertising Alliance (DAA) released its mobile privacy code of conduct for its members, titled "Application of Self-Regulatory Principles to the Mobile Environment;" and
3. Network Advertising Initiative (NAI) released its own Mobile Application Code governing its members' third-party behavioral advertising and reporting.

Three Consensus Points

The release of these three codes adds more layers—and hence additional competing standards—to the existing patchwork landscape of mobile privacy laws and standards. Perhaps most noticeably, the three codes provide three different sets of guidance on how mobile apps can clearly and effectively communicate their data collection, use and sharing practices to consumers. At the same time, the codes share a number of important principles, and together may facilitate the development of industry consensus on several points, including:

1. An emphasis on disclosing behavioral advertising and other third-party, cross-app collection and use of personal data;
2. The display of an app's privacy disclosures in a way that is more consumer-friendly—and more focused on what a typical consumer might most want and need to know—than the standard long-form privacy policy;
3. The expansion of covered data beyond core personally identify information ("PII") to account for the increasingly diverse and sensitive data collected by mobile apps, including precise geolocation, health data, and call or text logs.

Three Themes for Consideration

These three voluntary codes exemplify and expand on several themes in the developing mobile terrain that will be important for businesses to monitor in assessing their own mobile practices.

1. Data privacy and security practices are moving beyond initial "kitchen sink" privacy policies, often focusing on tailoring consumer notice and consent to different technologies—with much more limited screen real estate and consumer usage patterns—as well as to varying consumer expectations arising from different types of data collection and data usage.
2. Two of the codes reinforce the practical reality that multiple entities are involved in mobile data collection through a

single app. Thus, responsibility for consumer notice and consent must be shared among all entities in the mobile sphere, and the division of that responsibility remains an important and debated issue.

- Each of these codes recognizes precise geolocation as sensitive information to be accorded special attention and protections. As a corollary to that point, implicit in these codes' provisions is the acknowledgement that not all data is created equal—particularly sensitive data, in addition to the traditional categories of personally identifiable information, may require heightened consumer protection.

Each contribution to the recent mobile developments has different responses to these concerns. However, these major themes are a common refrain for mobile privacy and will likely shape future regimes and expectations. Businesses should be mindful of these distinctions as they consider their own data practices and as they consider whether to participate in any voluntary mobile practices code.

Conclusion

Although the three codes are voluntary, companies should consider whether they want to attempt to comply with any of the codes or related recommendations. The Federal Trade Commission (“FTC”) has indicated that it considers a company’s failure to abide by a self-regulatory program the company affirmatively agrees to adopt to be a deceptive trade practice in violation of Section 5 of the FTC Act. Notably, the DAA and NAI codes will be binding on all members of those organizations.

Contact Us



Mary Ellen Callahan, Partner, Jenner & Block

Phone: 202 639-6064 Email: mecallahan@jenner.com [Download V-Card](#)

Practices: [Privacy and Information Governance](#); [Content, Media & Entertainment](#); [Litigation](#)



Michael T. Borgia, Associate, Jenner & Block

Phone: 202 639-6033 Email: mborgia@jenner.com [Download V-Card](#)

Practices: [Privacy and Information Governance](#); [Litigation](#)



David M. Didion, Associate, Jenner & Block

Phone: 202 639-6082 Email: ddidion@jenner.com [Download V-Card](#)

Practices: [Privacy and Information Governance](#); [Litigation](#)



Sabrina N. Guenther, Associate, Jenner & Block

Phone: 312 940-7299 Email: sguenther@jenner.com [Download V-Card](#)

Practices: [Privacy and Information Governance](#); [Litigation](#)