wiley

NEWSLETTER

Privacy Pitfalls: Do Your Apps Know Too Much Information?

May 2011

As broadcasters and other new media companies continue to use smartphone applications and online services to expand their potential audiences, a federal prosecutor is exploring whether some applications illegally collect and share personal information. A federal grand jury in New Jersey apparently is investigating whether app publishers properly disclose the full extent of their data collection and sharing practices.

Streaming music provider Pandora disclosed in a recent Securities and Exchange Commission filing that it and other smartphone app publishers received subpoenas about their practices in early 2011.

Prosecutors appear to be focused on whether such data collection practices violate the Computer Fraud and Abuse Act (CFAA), an antihacking law passed in 1994, long before the recent iPhone-fueled proliferation of mobile apps. The Act prohibits a person or company from knowingly, and with the intent to defraud, exceeding authorized access to devices with storage capabilities. Thus, prosecutors could be proceeding under a theory that app publishers exceed their authority to access personal information via smartphones, as users granted only limited authority to publishers when they downloaded apps. Some mobile app publishers may be harvesting personal information, location information and financial account details made available through apps. Prosecutors are perhaps inclined to view such data collection, if undisclosed, as an indicator of a knowing intent to defraud.

Notably, the CFAA *does not* prevent broadcasters or other publishers from using a smartphone app or other online service to collect and share personal information. Rather, it focuses on whether such

Authors

Ari Meltzer
Partner
202.719.7467
ameltzer@wiley.law

collection exceeds authorized access and amounts to fraud.

Also, it remains to be seen whether prosecutors will proceed further than seeking subpoenas from mobile app providers. Prosecutors may find it difficult to actually establish a CFAA violation. In 2001, federal courts in New York and California rejected civil lawsuits claiming that installing cookies on computers violated the CFAA, holding that individual damages did not exceed the $5,000 threshold required for a CFAA claim.

Yet, to avoid potential liability under the CFAA, broadcasters should conduct a thorough review of how they collect, use and share personal information via mobile apps and other online services. Such a review should examine whether published privacy policies reflect actual data usage practices and are reasonably comprehensive, easy to read and easy to access.

*District of Columbia Bar pending. Supervised by principals of the firm.