e-commercelaw&policy

Mobile privacy in the US: recent developments

On 11 October 2012, the US Government Accountability Office (GAO) issued a report titled 'Mobile Device Location Data: Additional Federal Actions Could Help Protect Consumer Privacy.' Requested by Sen. Al Franken (D-MN), the Report recognises the efforts of Federal agencies to protect consumer privacy when using mobile devices but calls for additional action. Recent developments in the US mobile privacy field have also seen regulatory action by both the House of Representatives and the Senate. Mark W. Brennan, an Associate at Hogan Lovells LLP, presents two reports on these developments; Christopher Wolf, Partner at Hogan Lovells, co-authored the first of these.

New GAO Mobile Privacy Report Recommends Additional Federal Action

The GAO report is a reminder that app developers and other members of the mobile wireless ecosystem should review their existing data privacy and security practices for compliance with applicable Federal and state laws, especially as they deploy new consumer-oriented services.

Building on several other recent efforts to examine mobile device privacy and security issues, the Report examines three questions:

(1) How mobile companies in the mobile wireless ecosystem collect location data, why they share these data, and how this affects consumers;

(2) The types of actions that private sector entities have taken to protect consumers' privacy and ensure the security of location data; and

(3) The actions that Federal agencies have taken to protect consumer privacy and what additional Federal efforts, if any, are needed.

The Report emphasises that the collection, use, and sharing of location data carries both benefits and risks. Benefits can include providing improved services, facilitating compliance with legal requirements (such as enhanced 911 regulations), and targeted advertising. Risks can include the unexpected sharing of data with third parties, identity theft, threats to personal safety, and surveillance.

The Report also evaluates the policies of fourteen companies from the mobile wireless ecosystem in the following categories: (1) disclosures to users about data collection, use, and sharing; (2) user controls over location data; (3) data retention and safeguards; and (4) accountability. It found that companies disagree on whether location data is personal information. Apple, for example, classifies location data as

'nonpersonal information,' T-Mobile considers location data to be 'personally identifiable information,' and four companies indicated that whether location data constitutes personal information depends on factors such as 'how precise the data are and whether they are combined with other information about the user.'

Companies also differ in how much they inform users about how location data will be shared with third parties. The Report notes that some companies ensure that third parties comply with the company's privacy practices, whereas one company expressly disclaimed liability for any third party's failure to adequately protect shared data. Moreover, it is not always clear how companies gain users' consent to sharing their location data. The Report notes that this raises concerns with whether consumers are providing consent without complete knowledge of how their data will be used.

According to the Report, data retention policies also vary widely. Some companies keep data for only a few days, others retain data for a few years, and at least three companies keep location data indefinitely.

The Report also highlights recent contributions from other Federal agencies, including the Federal Communications Commission (FCC), Federal Trade Commission (FTC), and the Department of Justice. It also notes the efforts of the National Telecommunications and Information Association (NTIA), another federal agency that is conducting a privacy multistakeholder effort to develop a voluntary, enforceable code of conduct for mobile application transparency[2].

The report concludes with two recommendations for executive action:

1. NTIA should provide specific information regarding its procedures, deliverables, and time frames for its multistakeholder process. Additionally, NTIA should include a mechanism for enforcing adoption of and compliance with the principles that ultimately emerge from its process.

2. The FTC should publish comprehensive industry guidance on its views of appropriate actions by mobile companies with regard to privacy.

This Report is the latest in a series of recent efforts to examine mobile device privacy and security issues. In September 2012, the GAO issued a related report on mobile device security titled 'Information Security: Better Implementation of Controls for Mobile Devices Should Be Encouraged.'[3] Also in September 2012, the FTC issued a set of truth-in-advertising and privacy guidelines for mobile device application developers titled 'Marketing Your Mobile App: Get It Right from the Start.'[4] And in March 2012, the FTC issued its report on 'Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers.'[5] In that report, the FTC called on 'entities involved in the mobile ecosystem to work together to establish standards that address data collection, transfer, use, and disposal, particularly for location data.'

US Legislators and Regulators Continue to Focus on Mobile Privacy Concerns

Lawmakers and regulators on both US coasts continue to focus their attention on mobile privacy. In December, the US Senate Judiciary Committee approved a

measure that would establish legal requirements for applications (apps) that collect or share location information from mobile devices. A Democratic member of the US House of Representatives also released for public comment the first of three provisions that he plans to incorporate into a mobile privacy bill. And in California, Attorney General Kamala Harris filed a complaint alleging that Delta Air Lines violated California privacy law by failing to conspicuously post a privacy policy for its 'Fly Delta' app.

Mobile Privacy in the US Senate

On 4 December 2012 Senator Al Franken (D-MN), chairman of the Senate Subcommittee on Privacy, Technology, and the Law released a revised version of the Location Privacy Protection Act (Act)[6]that would require companies to obtain express consent from users before collecting, recording, obtaining, or sharing geolocation information from mobile devices.

Like the version of the bill that Franken introduced in 2011, the Act applies to the collection of location information from smartphones, laptops, tablets, in-vehicle navigation devices, and any other devices intended to be carried by or travel with users. Companies collecting location information without consent would be liable for civil penalties of no less than $2,500.

The Act allows companies to obtain one-time approval from users rather than having to obtain permission every time location information is collected or shared. The Act also specifies that it does not apply to disclosures for fire, medical, public safety, or other emergencies; disclosures pursuant to court orders supported by a showing of compelling need; and requests by law enforcement.

The Senate Judiciary Committee approved the Act on 13 December, even though Senators Charles Grassley (R-IA), Charles Schumer (D-NY), and Sheldon Whitehouse (D-RI) expressed concerns that the Act needs work to ensure that it does not stifle innovation. The full Senate did not consider the bill before the 112th Congress came to a close, but Franken has vowed that he would reintroduce the legislation in the 113th Congress.

Mobile Privacy in the House

Between 5 December and 3 January, House Democrat Hank Johnson of Georgia released three provisions for his planned AppRights.us bill that would address mobile app transparency, security, and control[7]. AppRights.us is a web-based project initiated by Johnson to develop mobile privacy legislation. Each provision of the bill was released for a two-week public comment period, and the congressman will report on the feedback he receives before introducing the bill.

The first of the three provisions addresses user control. It requires that developers enable users to delete mobile applications and the personal information stored by mobile applications at any time. Developers would also be prohibited from using or sharing personal information collected via deleted mobile applications within a reasonable time after the applications are deleted.

The second provision requires app developers to take reasonable measures to prevent unauthorised access to both personal and anonymous data.

And the third provision addresses mobile app transparency through notice and choice. It would require developers to notify users of the categories of data to be collected, the purposes for which data will be used, and the types of third parties to whom data will be disclosed.

Mobile Privacy in California

At the state level, California Attorney General Kamala Harris filed a privacy suit on 6 December against Delta Air Lines Inc., alleging that Delta's 'Fly Delta' app violates California law because it does not contain a privacy policy[8]. The complaint is California's first legal action against a mobile app developer under the California Online Privacy Protection Act of 2003 (CalOPPA). Harris seeks to enjoin Delta's distribution of the app; obtain penalties of up to $2,500 per app download; and recover investigation costs, attorney's fees, and other court costs.

As background, CalOPPA requires operators (i.e., owners) of commercial web sites or online services that collect personally identifiable information (PII) on California residents who use/visit the web sites or online services to 'conspicuously post' a privacy policy. The Attorney General's office has taken the position that mobile apps that use the internet to collect PII are 'online services' subject to CalOPPA. California's population size makes it safe for most app developers to assume that California residents comprise at least a portion of the app's download audience.

In October, Harris notified dozens of developers that they were not in compliance with the notice provisions of CalOPPA and gave them 30 days to bring their apps in line with the CalOPPA provisions.

The 'Fly Delta' app allows users to check in for flights, view and change their reservations, track their baggage, rebook flights, access frequent flyer accounts, and manage other information related to their travels. Harris claims that the app collects personal information from travelers, including location information and account numbers. 'California law is clear,' Harris said, 'Mobile apps collecting personal information need privacy policies.'

The suit is a reminder to companies that they should regularly review their mobile apps for compliance with rapidly evolving Federal and state laws.

Chris Wolf Partner

Mark W. Brennan Associate

Hogan Lovells, Washington DC Office

Christopher.wolf@hoganlovells.com

Mark.brennan@hoganlovells.com

A special thank you to James Denvil and Paul Otto for their assistance in preparing these articles.

1. Mobile Device Location Data: Additional Federal Actions Could Help Protect Consumer Privacy, Government Accountability Office Report 12-903 (Sept. 2012), available at http://www.gao.gov/assets/650/648044.pdf.

2. See National Telecommunications & Information Administration, Privacy Multistakeholder Process: Mobile Application Transparency, at http://www.ntia.doc.gov/other-publication/2012/privacy-multistakeholder-process-mobile-application-transparency; see also National Telecommunications & Information Administration, July 12, 2012 Privacy Multistakeholder Meeting: Details (June 26, 2012), at http://www.ntia.doc.gov/other-publication/2012/july-12-2012-privacy-multistakeholder-meeting-details ("The objectives of the July 12, 2012 meeting are to: 1) promote discussion among stakeholders concerning mobile app transparency by employing a structured, open process; and 2) provide a venue for stakeholders to agree on the schedule and format of future meetings").

3. Information Security: Better Implementation of Controls for Mobile Devices Should Be Encouraged, Government Accountability Office Report 12-757 (Sept. 2012), available at http://www.gao.gov/assets/650/648519.pdf.

4. See http://business.ftc.gov/documents/bus81-marketing-your-mobile-app

5. FTC Report, 13-14 (Mar. 2012), available at http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

6. S. 1223, 113th Cong. (2012).

7. https://apprights-hankjohnson.house.gov/

8. http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-files-suit-against-delta-airlines-failure