Consumer Protection is your Smartphone too smart?

Smartphone tracking of consumers locations will test the boundaries of the Computer Fraud and Abuse Act

By William E. Viss

The smartphone in your briefcase is probably tracking and storing your location. As a consumer, you may enjoy this feature and even pay a premium to enhance its use. However, other smartphone owners are less impressed. They feel the manufacturers' failure to disclose that such tracking occurs violates their privacy rights and constitutes fraud.

To mobilize these claims, unhappy con- sumers are turning to an old favorite — the Computer Fraud and Abuse Act (CFAA), 18
U.S.C. § 1030. The CFAA makes it unlawful for a person to access a protected computer without authorization, or to exceed autho- rized use. But does that mean mobile device manufacturers are guilty of a federal crime or subject to civil penalties for tracking a user's location without the user's consent? At least two Apple product owners say they are, and have filed a complaint to that effect. As a result, the courts are once again asked to determine the limits of the CFAA.

Viss is an associate with Archer & Greiner P.C. in Haddonfield. He is a mem- ber of the firm's commercial litigation department and concentrates his practice in litigation services.

The Complaint

On April 22, plaintiffs Vikram Ajjam- pur, a Florida resident, and William Devito, a resident of New York state, filed a complaint in the United States District Court, Middle District of Florida, seeking class-action status and naming Apple, Inc., as the sole defendant. Ajjampur owns the iPhone, De- vito the 3G iPad. Both claim they travelled extensively with their devices, but were un- aware their locations were being tracked and stored. Due to the plaintiffs' travels to nu- merous states, they also assert Apple's track- ing policy violated not only the CFAA, but also infringed upon antifraud statutes of the states they visited, including the New Jersey Consumer Fraud Act, N.J.S.A. §§ 56:8-1 et seq.
At the heart of the plaintiffs' complaint lie Apple's alleged privacy violations. Cit- ing various Internet articles for support, the plaintiffs contend that the mobile devices "log, record and store users' locations" and "download the user location data to the us- er's computer when the mobile device syn- chronizes ('syncs') or shares data with the computer." The plaintiffs further allege that Apple collects the users' location informa tion "covertly, surreptitiously and in viola- tions of law" and in "conjunction with other businesses that develop applications for Apple's devices" without obtaining a con- sumer's informed consent.

In particular, the plaintiffs assert that because mobile Apple products such as the iPhone and the iPad travel with the user at all times, the information collected by Ap- ple is highly personal: "[I]ndeed, in many instances it may be information to which employers and spouses are not privy." The plaintiffs warn that making such information publicly available "places users at serious risk of privacy invasions, including stalk- ing." They further contend that the tracking caused them harm "because they were per- sonally tracked just as if by a tracking device for which a court-ordered warrant would or- dinarily be required," and therefore demand that the court require Apple to reconfigure its tracking software in order to avoid collect- ing personal location information, or sync- ing the information with other computers.

The Boundaries of the CFaa

The complaint is one of many recent civil actions that will test the metes and bounds of the CFAA. Originally passed in
1986, the act was intended to curb computer hacking in the stricter sense of the word. See S. Rep. No. 99–432 at 2–3 (1986). At that time, regular use of computers was a recent phenomenon. As the number of computer crimes

increased, Congress realized the cur- rent laws were insufficient to address un- lawful acts involving new technology and responded accordingly.

NEW JERSEY LAW JOURNAL, JULY 25, 2011

The resulting CFAA is a powerful statute supporting both criminal and civil causes of action. The civil remedy provides that any- one who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . informa- tion from any protected computer" commits an unlawful act and may be held liable for damages, injunctive, or equitable relief. 18 U.S.C.A. § 1030 (a)(2)(C) & (g). The term "exceeds authorized access" is defined by the act to mean gaining "access to a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C.A. § 1030(e)(6).

Over the years, litigants have devel- oped a number of uses for the CFAA, some of which fall well outside the act's intended purpose. Such cases have arisen in employ- ment contexts, for example, where employees were in violation of the employer's computer policy, either because they had been termi- nated and therefore no longer had authority to access the employer's computer system, or simply because the employees visited person- al websites during business hours. By citing the CFAA in those instances, the complaining party essentially straps the civil remedy pro- vision of the Act to an otherwise run-of-the- mill claim, and proceeds to court armed with a federal criminal statute.

While most courts tend to disallow the use of the CFAA in this way, see *Lee v. PMSI, Inc*., 8:10-cv-2904 (order filed May6, 2011)(ruling that employee's use of em- ployer's computer to access Facebook on company time did not violate CFAA), others have shown a willingness to expand the Act's reach. See *U.S. v. Rodriguez,* 628 F.3d 1258 (11th Cir. 2010)(affirming conviction and 12-month prison sentence of Social Security Administration employee found to have vio- lated the CFAA by using government data- base for personal use in violation of employ- ment policy).

In one of the more alarming opinions, the Ninth U.S. Circuit Court of Appeals held that when an employee has knowledge of an em- ployer's computer-use restrictions, any breach of the computer policy exceeds authorized use and subjects the employee to the full force of the CFAA. See *U.S. v. Nosal*, 10-10038, 2011 WL 1585600 (9th Cir. Apr. 28, 2011). Thank- fully, the dissent in *Nosal* was quick to point out that the majority's holding essentially criminalizes millions of employees who use work computers innocuously "to access their personal email accounts or to check the lat- est college basketball scores." It appears that if the CFAA were consistently applied as the majority in *Nosal* suggests, it would not only stretch the CFAA to a breaking point, but also stifle fantasy football leagues nationwide. Clearly, this was not Congress' intent.

Future Developments

It is less clear, however, whether the CFAA is properly applied in the case of smart- phones tracking a user's physical location. As described above, recent case law applying the act in other contexts is somewhat scattered. This is the result of the courts' willingness to stretch the act beyond its intended reach in an effort to accommodate litigants who bolt the CFAA to claims involving computers of any kind. To a certain extent, this is the cycle we expect. The market presents a popular prod- uct that arguably infringes upon a consumer's legitimate privacy concerns, and the law is forced to respond. However, from a practical perspective, simply cloaking an allegation in "exceeding authorized access" language un- der 18 U.S.C.A. § 1030(e)(6), should not au- tomatically arm a litigant with a CFAA claim. Nor is it likely that Congress intended its anti- hacking act to criminalize smartphone manu- facturers for tracking and storing a user's lo- cation. This is especially true where a party has access to more appropriate legal remedies in the form of federal privacy protections, state antifraud or consumer protection acts, or traditional common-law tort claims.

What is certain, is that privacy rights are at issue and many government officials are concerned. For example, the Federal Com- munications Commission scheduled a June 28 public education forum designed to ex- plore how "consumers can be both smart and secure" when using advanced mobile devices. While, in New Jersey, federal prosecutors are investigating whether an online music ser- vice provider, Pandora Media, Inc., violated the CFAA by transmitting information con- cerning a user's age, gender and location to third-party vendors. It is in this context that the Middle District of Florida must determine the boundaries of the CFAA as it applies to smartphones. The court's analysis will no doubt involve deciphering Congress' original intent, and balancing a consumer's right to privacy against the growth of a robust market with the collection and distribution of

users' personal information at its core. This is a dif- ficult task and one that will no doubt further define the boundaries of the CFAA. ■