Recent Legal Consequences for Spyware Users

Richard Raysman and Peter Brown, New York Law Journal

December 9, 2014

Richard Raysman and Peter Brown

ljh

Spyware, which is broadly defined as software that aids in gathering information about a person or organization without their knowledge, is considered an increasingly vexing problem. Spyware programs assist users in spying on partners in intimate relationships, circumventing restrictions designed to protect copyright content and stealing personally identifiable information, among other capabilities. The Federal Trade Commission (FTC) has estimated that 27.3 million Americans have been victims of identity theft, which is closely associated with spyware, and such losses to businesses and financial institutions therefrom are approximately $48 billion dollars.

Source: http://www.newyorklawjournal.com/id=1202678228155/Recent-Legal-Consequences-for-Spyware-Users

In response, federal prosecutors, state attorneys' general, federal courts, companies and even non-governmental organizations (NGOs) are taking concerted action. For instance, just last month, a human rights group began to offer a tool to allow individuals to determine whether their electronic devices are being monitored by governmental entities by spyware. At the state level, rent-to-own retail company Aaron's was required to pay upwards of $28 million in a settlement with the California Attorney General. Aaron's had been accused of violating California's unfair commercial practices and privacy laws in part because it had installed a spyware feature on its' customers computers named "Detective Mode," a program that allowed Aaron's franchise employees to surreptitiously monitor the customer's computer remotely.

Courts and other elements of the judicial and criminal justice systems have dealt with cases involving spyware in which plaintiffs allege a distinct variety of causes of action. This article will discuss that variety, as well as: how a federal privacy and anti-wiretapping statute was applied when a disgruntled husband installed spyware on his estranged wife's computer; one of the first instances of a grand jury indicting purveyors of spyware on criminal charges; and why falsely accusing a competitor of trafficking in spyware can engender a suit against the accuser for defamation.

Spyware and Estranged Spouses

Leo Tolstoy once observed that "all happy families are alike; each unhappy family is unhappy in its own way." One such unhappy family was recently in federal court in Louisiana based upon allegations that the husband had installed spyware on his wife's computer during the pendency of their divorce proceedings. See *LaRocca v. LaRocca*, No. 13-4748, 2014 WL 5040720 (E.D. La. Sept. 29, 2014).

After the wife (Mrs. LaRocca) had initially filed for divorce in 2011, she remained in those prolonged proceedings with her ex-husband (Mr. LaRocca) two years later. Mrs. LaRocca then learned that her husband had installed spyware onto her computer without her knowledge. She alleged that doing so was in violation of the Electronic Communications Privacy Act (ECPA). See 18 U.S.C. §2510. Discovery conducted during the parallel divorce proceedings exposed that Mr. LaRocca had installed a spyware program on his estranged wife's computer that contained features, among others, that allowed the purchaser to "create a complete record of personal computers and Internet activity."

Mr. LaRocca admitted to installing the spyware, but averred that he was nonetheless immune under the ECPA based on the "interspousal exception" first announced in *Simpson v. Simpson*, 490 F.2d

803 (5th Cir. 1974). *Simpson* refused to find a husband liable by holding that the Federal Wiretap Act, a statute that was later amended by the ECPA, was not designed to apply to a husband's actions in wiretapping his wife's phone calls absent her permission or awareness. Simpson declined to apply the ECPA to "purely personal actions such as one between spouses on the grounds that such actions were not contemplated or intended by Congress."

Although it conceded the prima facie resemblances between the two cases, the court in *LaRocca* distinguished *Simpson* en route to holding that the "interspousal exception" did not apply. First, the court observed that, unlike in *Simpson*, the LaRocca's had already initiated divorce proceedings. Given the commencement of divorce proceedings, through the use of spyware Mr. LaRocca was able to glean not simply evidence of philandering, but also privileged communications between Mrs. LaRocca and her attorney. Second, and more important, Mr. LaRocca collected *all* data from his estranged wife's computer, and not just telephone conversations. Ultimately, as the information gained through the installation of spyware "is different and broader in scope than the information gained through listening in on phone calls," and tends to "erode the increasingly discredited conclusions in *Simpson*," the assertion of the interspousal exception was rejected.

LaRocca reflects how the evolution of technology, in particular how it now affords the ability to collect copious amounts of data of unwitting individuals at any time, has fundamentally altered courts' approach to privacy cases. As spyware epitomizes such a capability, it is unsurprising that authorities have now adopted a more serious approach to neutralizing its often insidious effects, as the criminal indictment discussed below encapsulates.

Selling a Spyware Mobile App

September 2014 brought one of the first-ever criminal cases filed against a distributor of a spyware mobile application (app). In *United States v. Akbar*, Complaint, Crim. No. 1:14-cr-276 (E.D. Va. Sept. 29, 2014) federal prosecutors announced that criminal charges would be brought against the defendant (Akbar) for violations of 18 U.S.C. §2512. This statute prohibits the "manufacture, distribution, possession and advertising of wire, oral, or electronic communication intercepting devices." Akbar was additionally charged with a conspiracy to violate this provision. See 18 U.S.C. §371.

Akbar had created StealthGenie, a spyware app that according to the government had been illegally intercepting wire and electronic communications made using smartphones. Once installed on the

target's smartphone, Stealth Genie permitted the purchaser to record all incoming and outgoing calls of the target's smartphone, intercept all of those calls, and monitor the target's text messages and emails. The app was undetectable to a normal smartphone user, and purchasers could intercept the target's communications in real time, as the app was synced with a server hosting StealthGenie's website. Such a use was of a benefit to the purchaser, as the purchaser would thus only need a few minutes in physical control of the smartphone to gain access to subsequent monitoring of the device virtually ad infinitum.

StealthGenie used its website, which included fictitious testimonials, to market and sell the app. Among other unsavory details, Akbar marketed StealthGenie to prospective purchasers who suspected a spouse or romantic partner of infidelity. According to StealthGenie's business plan, the "[s]pousal cheat" market would likely constitute 65 percent of Stealth Genie purchasers.

With respect to 18 U.S.C. §2512, the indictment charged that Akbar: (1) sold an app while knowing that the design rendered was "primarily useful for the purpose of surreptitious interception of wire and electronic commerce;" (2) disseminated by electronic means an advertisement for such an app that was for these illegal purposes; and (3) disseminated by electronic means an advertisement to promote the use of the app for such purposes.

The facts alleging conspiracy to violate 18 U.S.C. §2512 are perhaps more interesting, as they shed insight both on how spyware companies are able to insidiously invade the privacy of unwitting individuals, or aid and abet others with identical motives, and how the government approached the accumulation of sufficient factual predicates to secure a grand jury indictment. Such overt acts to further the conspiracy cited in the complaint included: Akbar sending the source code for StealthGenie to an unnamed co-conspirator, and creating then disseminating a number of advertisements for StealthGenie via its eponymous website. What potentially sealed Akbar's fate occurred when he and his co-conspirators sold the Android version of StealthGenie to an undercover FBI agent and thereafter intercepted communications on the smartphone that were later made available on the StealthGenie website.

Of most interest in the facts listed to buttress the conspiracy claim is the emphasis on Akbar's methods and deployment of advertising, likely because StealthGenie is different than typical spyware insofar as it is a third party that installs the spyware on the target device, and not the unwitting user as is customarily the case. Ergo, proving causality is different, as Akbar is one step

Source: http://www.newyorklawjournal.com/id=1202678228155/Recent-Legal-Consequences-for-Spyware-Users

removed from the actual cause of the subsequent use of the smartphone to effectuate an illegal interception of the communications.

Spyware Defamation Case

As the cases above prove, selling, advertising, and installing spyware can potentially engender criminal or civil liability. Additionally, as a recent case in the Southern District of New York shows, liability can also be incurred by parties who accuse others of using spyware. See *Broadspring v. Congoo*, No. 13-CV-1866 (JMF) (S.D.N.Y. Aug. 20, 2014). Broadspring centered on a highly rancorous and prolonged dispute between "bitter rivals" in the online advertising industry, Broadspring and Congoo. The two companies each operated online advertising networks and competed to place their customers advertisements on websites referred to in this context as "publishers."

Broadspring had discovered that the Senior VP of Business Development for Congoo (Cosentino) had been pseudonymously posting in Internet forums that Broadspring was formerly "Mindset Interactive, a notorious spyware company." Cosentino added that Mindset was founded by an individual who came to be known as "Spamford Wallace" and that it was shut down by the Federal Trade Commission (FTC) in 2005 after it was caught distributing spyware.

Contemporaneously, Cosentino had disseminated similar statements to publishers that had worked with Broadspring, such as the New York Daily News and Geology.com. Geology.com had given Broadspring the exclusive right to serve advertisements on its site. After Cosentino saw the Broadspring-facilitated advertisements on Geology.com, he called the principal of the site and informed him that he "could get in trouble running those ads." According to Cosentino, Broadspring had "gotten in trouble for spyware" and had been "in court over something." Upon hearing this news, Geology.com terminated its dealings with Broadspring, *even though* it had been in the midst of replacing Congoo's advertisements with Broadspring advertisements.

A mere few weeks later, Broadspring sued Congoo for false advertising under the Lanham Act, defamation, and tortious interference with contract. In support of its motion for summary judgment on the defamation claim, the defendants argued for immunity because the statements at issue constituted protected opinion under the First Amendment. In analyzing the First Amendment claim, the court applied the relevant test to distinguish between constitutionally protected expressions of opinion and actionable assertions of fact. The test asks whether a reasonable judge could conclude that the statement declares or implies a provably false assertion of fact. In the instant case, the

judge determined there was "no question" that the defendants' statements imply provably false assertions, as neither Broadspring or Mindset had ever been shut down by the FTC, nor had it been founded by "Spamford Wallace." Therefore, the defendants' motion for summary judgment on the defamation claim was denied.

Conclusion

The first recorded use of the word spyware came in an Internet forum in 1995 and it referred to software meant for espionage. In the nearly 20 years since, spyware has proliferated to the point where it is considered a common pejorative in the software industry that encompasses cyber spying, employee monitoring software, and various forms of espionage. Elsewhere, in an undoubtedly novel use of spyware, employees at two high schools in suburban Philadelphia implanted spyware on school-issued laptops to remotely activate webcams embedded in the laptops.

As spyware is now disseminated in multifarious ways, the legal system has begun to respond to each of the disparate problems that arise as a result. From indicting foreign nationals who sell mobile apps containing spyware, to sanctioning those who falsely accuse competitors of using spyware, judges and prosecutors will have to continue to be flexible in combatting the threat of spyware.

Richard Raysman is a partner at Holland & Knight and Peter Brown is the principal at Peter Brown & Associates. They are co-authors of "Computer Law: Drafting and Negotiating Forms and Agreements" (Law Journal Press).

Source: http://www.newyorklawjournal.com/id=1202678228155/Recent-Legal-Consequences-for-Spyware-Users