



Those iPad Hackers Were Probably Seeking Publicity, Not Profit

February 9, 2011

The two iPad hackers who obtained the personal data of approximately 120,000 iPad users [by exploiting a security weakness](#) in AT&T's resubscription page are now facing federal charges and potential jail time.

After the hackers publicized their activities, the FBI started an investigation that ended with criminal charges against the hackers. The hackers were charged with conspiracy to access a computer without authorization and with fraud for intending to use the personal information that was collected. The charges are that they collected the usernames, e-mail addresses, billing addresses, and passwords of AT&T customers through their computer program and intended to profit from the personal data.

A review of case law under the relevant statute shows that there have been a limited number of cases with these types of charges. Further, the complaint itself alleges that the hackers used the information to e-mail board members of multiple news outlets. The e-mails noted that personal data had been taken from an unsecured AT&T server, adding, "If a journalist in your organization would like to discuss this particular issue with us, I would be happy to describe the method of theft in more detail."



This suggests that the hackers' goal was probably publicity rather than profit. They were interested in getting their story out — and any attempt to profit from the data was, at most, a secondary consideration, which may not satisfy the statutory requirement of unauthorized access to a computer “with intent to defraud.”

Moreover, the statute itself exempts any unauthorized access where the only thing obtained was the use of a computer and the value of such use was less than \$5,000 per year. Here, although the hackers did discuss selling the information, it is still highly questionable whether their actions reached the requisite dollar threshold. The prosecutors say AT&T has spent approximately \$73,000 to remedy the security breach. That cost was not caused by the hackers, however, because the security breach was always there and the hackers merely identified its existence. Either way, AT&T needed to fix the security breach and had to pay that sum in any case.

Despite any weaknesses in the prosecution's case, the publicity given to the hackers' feat probably encouraged the authorities to press charges and thereby reassure the public that Internet security is safe and that all violators will be held accountable.

Crime in the Suites is authored by the [Ifrah Law Firm](#), a Washington DC-based law firm specializing in the defense of government investigations and litigation. Our client base spans many regulated industries, particularly e-business, e-commerce, government contracts, gaming and healthcare.

The commentary and cases included in this blog are contributed by Jeff Ifrah and firm associates Rachel Hirsch, Jeff Hamlin, Steven Eichorn and Sarah Coffey. These posts are edited by Jeff Ifrah and Jonathan Groner, the former managing editor of the Legal Times. We look forward to hearing your thoughts and comments!