

PATRICK J. LEAHY, VERMONT, CHAIRMAN

HERB KOHL, WISCONSIN
DIANNE FEINSTEIN, CALIFORNIA
CHARLES E. SCHUMER, NEW YORK
RICHARD J. DURBIN, ILLINOIS
SHELDON WHITEHOUSE, RHODE ISLAND
AMY KLOBUCHAR, MINNESOTA
AL FRANKEN, MINNESOTA
CHRISTOPHER A. COONS, DELAWARE
RICHARD BLUMENTHAL, CONNECTICUT

CHARLES E. GRASSLEY, IOWA
ORRIN G. HATCH, UTAH
JON KYL, ARIZONA
JEFF SESSIONS, ALABAMA
LINDSEY O. GRAHAM, SOUTH CAROLINA
JOHN CORNYN, TEXAS
MICHAEL S. LEE, UTAH
TOM COBURN, OKLAHOMA

United States Senate

COMMITTEE ON THE JUDICIARY

WASHINGTON, DC 20510-6275

BRUCE A. COHEN, *Chief Counsel and Staff Director*
KOLAN L. DAVIS, *Republican Chief Counsel and Staff Director*

April 12, 2011

The Honorable Lanny Breuer
Assistant Attorney General
Criminal Division
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530

Dear Assistant Attorney General Breuer:

This month, two independent events underscored our nation's need for stronger digital privacy protections. On Friday, April 1, one of the nation's largest digital marketing companies, Epsilon Data Management, LLC, announced that hackers had breached their security systems and stolen millions of consumers' email addresses. The following Monday, public securities filings revealed what appears to be an investigation by the U.S. Attorney's Office of New Jersey into allegations that certain smartphone applications were collecting sensitive consumer information and disclosing it to third parties unbeknownst to consumers. This information ranged from users' phone numbers to their friends lists to their geographic location. The alleged conduct in both cases will likely be investigated under a single statute called the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030. *See* Amir Efrati, Scott Thurm and Dionne Searcey, Mobile-App Makers Face U.S. Privacy Investigation, *The Wall Street Journal*, April 5, 2011.

These allegations raise broad questions about the need to better protect Americans' digital information and give them greater awareness and control over that information. They also highlight potential ambiguities and limitations of the CFAA which create uncertainties for industry and limit safeguards for consumers. In light of these incidents, we are writing to ask that you do everything possible to ensure that this specific statute is enforced effectively and transparently. Specifically, we ask that you clarify the Department's understanding of the scope of the CFAA's consumer protection provisions, update the Department's prosecutorial guidance for the statute, and indicate to us where additional funding or legislation may be needed.

First, while the hacking of Epsilon would appear to be a clear violation of the CFAA, the application of that statute can be ambiguous in other circumstances. In addition to covering outsider hacking activities, the CFAA also covers situations where an insider who already has access to a computer "exceeds authorized access" to obtain information from that computer. Where there is a privacy policy, employee contract, or other document laying out the scope of an individual or entity's authorization to access a computer, courts have found it easy to determine whether someone has exceeded their authorized access and violated the CFAA. *See, e.g. EF Cultural Travel BV v. Explorica*, 274 F.3d 577 (1st Cir. 2001) (defining scope of authorization based on a confidentiality agreement).

But where there *isn't* a document clearly laying out the scope of authorization, the law is more unclear. As the Department itself has acknowledged, federal circuits are split on the question of whether limits on authorized access can be inferred from the relationship between the user and the entity accessing the user's computer. *Compare EF Cultural Travel BV v. Zefer Corp.*, 318 F.3d 58 (1st Cir. 2003) (refusing to limit authority based on "reasonable expectations" test), *with United States v. Phillips*, 477 F.3d 215, 219 (5th Cir. 2007) ("Courts have... typically analyzed the scope of a user's authorization to access a protected computer on the basis of the expected norms of intended use or the nature of the relationship established between the computer owner and the user."). Because many smartphone apps lack privacy policies, many of the applications being investigated by the U.S. Attorney's Office may fall into this legal gray area.

We write to ask the Department to clarify how it determines the scope of authorization under the CFAA in the absence of a written policy or agreement addressing the issue. We further ask that the Department communicate this interpretation to consumers, prosecutors, and industry stakeholders. We believe that a clear statement on the application of the CFAA in these circumstances will help consumers know their rights, help industry develop new products and services, and help law enforcement take action against bad actors.

Second, we also think it is important for all prosecutors to be aware that the Computer Fraud and Abuse Act protects more than traditional desktop and laptop computers. The definition of "computer" in the CFAA is a broad one and the U.S. Court of Appeals for the Eighth Circuit recently reaffirmed that the CFAA protects smartphones and a broad range of other electronic devices. *See U.S. v. Kramer*, 2011 WL 383710 (8th Cir. 2011). We ask that the Department update its *Prosecuting Computer Crimes* manual to reflect this recent federal court precedent. Establishing that the CFAA covers smartphones and other electronic devices will help U.S. Attorneys and Department officials recognize and stop violations of the CFAA's modest protections.

Finally, we write to ask how we as the Senate can help you enforce this critical protection of Americans' security and privacy. Does the CFAA require updating in light of the Epsilon breach and the smartphone app allegations? Are there other areas of the law that should be enhanced to better protect digital privacy? Does the Computer Crime and Intellectual Property Section have the resources it needs to protect Americans from online criminals?

Your work is critical to Americans' digital privacy. We welcome the opportunity to support you in this important endeavor.

Sincerely,



Al Franken
United States Senator



Richard Blumenthal
United States Senator