

September 19, 2012

The Honorable Patrick J. Leahy
Chairman
United States Senate
Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Charles E. Grassley
Ranking Member
United States Senate
Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, DC 20510

Dear Chairman Leahy and Ranking Member Grassley:

We are writing today to support Chairman Leahy's amendment to H.R. 2471, a bill to amend section 2710 of title 18, United States Code. This amendment updates the Electronic Communications Privacy Act (ECPA) to provide protection to communications such as email, private social network posts, and other information stored in "the cloud." We believe information like email should have the same legal protection as letters or information held by an individual in their home. We urge all members of the Committee to support this amendment

When ECPA was drafted in 1986, there was no "World Wide Web," very few people carried a cell phone, almost nothing was stored in the "cloud," – a general term for information held by 3rd parties and accessed through the Internet – and social networking was still years away. E-mail was just starting to come into use and large companies were starting to transmit data to other companies to perform internal functions like payroll and data processing. ECPA was Congress's effort to deal with those new developments. But Congress has not substantially updated the law over the intervening years, despite the astounding way in which technology has overrun the world we once knew.

As society's presence online has increased, ECPA has been stretched to cover many of the new technologies Americans enjoy. Unsurprisingly, that stretch is an uncomfortable fit for the original law and it is now substantially out of date. While such a lack of privacy protection affects all Americans, minority communities, already disproportionately targeted by law enforcement, face particular burdens.

For example, a 2010 Freedom of Information Act (FOIA) request from the Electronic Frontier Foundation revealed that the Department of Homeland Security (DHS) monitored social

networking sites that cater to specific racial and ethnic demographics¹. The FOIA documents revealed that, during the days leading up to President Obama's inauguration, DHS had established centers to monitor the online African American community site BlackPlanet for specific "items of interest," including users' political beliefs and key words related to race. The same FOIA also discovered that U.S. Citizenship and Immigration Services had been monitoring social networking sites including MiGente, which caters to the Latin American community, to investigate citizenship petitions.

Similarly, in August 2011, an Associated Press report revealed a massive surveillance department established within the New York Police Department (NYPD) after 9/11 to monitor Muslim neighborhoods and infiltrate their community organizations². According to officials involved, undercover officers were sent out to investigate all parts of daily life in these communities including bookstores, bars, Internet cafes and clubs looking for "hot spots" of "radicalization." As part of a largely secret police program, they spied on and recorded the lives of innocent Americans without any evidence of wrong doing.

The NYPD has long viewed the Internet as dangerous territory. In a 2009 report it said:

"The Internet plays an important role during the radicalization process.... The Internet becomes a virtual "echo chamber" – acting as a radicalization accelerant while creating the path for the ultimate stage of Jihadization. In the Jihadization phase, people challenge and encourage each others move to action. The internet (sic) is now a tactical resource for obtaining instructions on constructing weapons, gathering information on potential targets, and providing spiritual justification for an attack."³

It is not known whether NYPD's efforts to track Muslims involved government surveillance under ECPA because of the secrecy of the program. Assuming ECPA applied, however, it is likely that the outdated nature of ECPA's protections would have allowed these activities to proceed with little transparency and judicial oversight.

For all of these reasons we support an update to ECPA and strongly urge members to support the Chairman's amendment to H.R. 2471.

Sincerely,

American Civil Liberties Union

American Muslim Voice

¹ Jennifer Lynch. "New FOIA Documents Reveal DHS Social Media Monitoring During Obama Inauguration." *Electronic Frontier Foundation*. October 13, 2010. Available at <https://www.eff.org/deeplinks/2012/08/tpp-creates-liabilities-isps-and-put-your-rights-risk>

² Highlights of AP's Pulitzer Prize-winning probe into NYPD intelligence operations. *The Associated Press*. Available at <http://ap.org/media-center/nypd/investigation>

³ Mitchell D. Silber. *Radicalization in the West: the Homegrown Threat*. *The New York Police Department*. 2009

Asian Law Alliance

Bill of Rights Defense Committee

Casa Esperanza

Center for Constitutional Rights

Center for Media Justice

Communications Workers of America

Council on American-Islamic Relations

DRUM- Desis Rising Up & Moving

Four Freedoms Forum

The Greater Cleveland Immigrant Support Network

Japanese American Citizens League

The Leadership Conference on Civil and Human Rights

Mexican American Legal Defense and Educational Fund

Muslim Advocates

Muslim Legal Fund of America

NAACP

National Hispanic Media Coalition (NHMC)

National Immigration Project of the National Lawyers Guild

National Urban League

OneAmerica

United Church of Christ, Office of Communication, Inc.

UNITED SIKHS