



# Spy in the Clouds: How DOJ Actions Could Harm U.S. Competitiveness Abroad

Steve Pociask \*

## Background

The Department of Justice (DOJ) issued a search (and seizure) warrant to Microsoft Communications to hand over the private email communications of a suspected drug trafficker. The only problems with the request, however, is that the drug suspect happens to reside in Ireland, the emails being sought are stored on an Internet server located in Ireland, and the server belongs to a subsidiary of Microsoft that operates in Ireland. Does the U.S. have any legal right to the personal information of foreign citizens? Does the U.S. have the right to compel a business in a foreign country to cooperate? What if a foreign country wanted your personal communications, should the U.S. comply?

Microsoft is currently engaged in a legal fight to prevent the release of these emails to the DOJ. Legal issues aside, there are strong economic reasons for why the DOJ request represents a bad and potentially costly practice for the U.S. economy. As this *ConsumerGram* will demonstrate, the fallout of the DOJ's legal overreach will heighten privacy concerns and distrust of American businesses operating abroad. The major risk is that it will encourage foreign citizens, companies and countries to stop doing business with U.S. companies operating overseas.

---

\* Steve Pociask is president of the American Consumer Institute Center for Citizen Research, a nonprofit educational and research organization. For more information about the Institute, visit [www.theamericanconsumer.org](http://www.theamericanconsumer.org).

As a response to this issue, Senators Hatch, Coons and Heller have just introduced *The Law Enforcement Access to Data Stored Abroad Act*.<sup>1</sup> To appreciate why Congress needs its full and immediate consideration of this legislation is to understand the immense economic repercussions at stake. As this ConsumerGram will discuss, the adverse consequences of the DOJ's actions could eventually cost U.S. companies over \$180 billion dollars per year and over two million jobs. It could also permanently stunt the U.S. leadership in the high-tech market for decades to come.

### **Harm to U.S. Interests Abroad**

When one country, such as the U.S., requests personal information, records and communications on a foreign citizen living overseas, adjudication of that request by the foreign country is based on existing agreements and treaties between the two countries. If the U.S., for example, tries to reach across a foreign boarder to seize the information of foreign citizens without approval of the foreign country, it is sidestepping existing cooperative agreements (such as Mutual Legal Assistance Treaties) between the U.S. and the foreign country, and therefore is violating these agreements and disregarding the basic sovereignty of that country.

These actions will likely lead to diplomatic tension, distrust and potentially retaliation by foreign leaders, which will affect future cooperation between the countries with respect to trade and other matters. In this case, it could affect the willingness of foreign citizens, companies and countries to do business with U.S. high-tech companies.

### **Customer privacy**

Countries have different privacy laws. These laws affect the collection, public availability, commercial use and retention of customer and business information. The European Commission expects their data protection rules to be respected. If the U.S. feels that

---

<sup>1</sup> Their news release is available online at <http://www.hatch.senate.gov/public/index.cfm/releases?ID=8e28c3f9-842b-4d96-83b7-9f71cf40bc07>.

it has rights to private information of citizens living abroad, this opens the door for foreign countries to prosecute companies who comply with that request or to ask American companies or foreign affiliates to turn over confidential data stored in the U.S.

Similarly, if the U.S. requests or subpoenas information on foreign citizens and companies residing overseas from U.S. multinational corporations or American subsidiaries that operate within foreign countries, not only is it circumventing existing agreements between the two countries, but it could also be putting U.S. companies that do business overseas in violation of the host country's privacy and espionage laws.

At a minimum, consumers and businesses overseas will have concerns and misgivings about doing business with U.S. corporations. This may lead these consumers and businesses to shun U.S. company products and services, and it could cause the host country to take steps to protect its citizens and companies. Furthermore, foreign countries could become concerned about spying on its leaders and espionage of state secrets, as has occurred with revelations of the NSA's recent PRISM spying scandal. The result could leave U.S. companies facing lost sales to consumers and small business, as well lost contracts with businesses and foreign governments.

### **Reprisals on U.S. Corporations Operating Abroad**

There is a lot at stake if countries retaliate or shun U.S. businesses. Worldwide, high-tech services and applications are valued at \$2 trillion per year, with U.S. companies being the major providers of software, security, data analytics, applications like search and online commerce, cloud computing and webhosting.<sup>2</sup> On the equipment side, the U.S. exported \$76 billion in telecommunications, semiconductor, computers and computer accessories in capital equipment in 2013.<sup>3</sup>

---

<sup>2</sup> "Cloud-Related Spending by Businesses to Triple from 2011 to 2017," HIS press release, February 14, 2014.

<sup>3</sup> Data is from the U.S. Census Bureau, U.S. Bureau of Economic Analysis, as of September 4, 2014.

Emails, like the ones residing in data centers in Ireland, are stored as part of cloud computing services – a service with business expenditures topping \$174 billion in 2014 and expected to increase three-fold in the next few years.<sup>4</sup> These services include a host of other consumer services, including customer service and retail applications, as well as services directly purchased by the banking, government, media, healthcare and manufacturing sectors. Among the top cloud computing companies are a long list of U.S. firms, including Amazon, Google, VMware, Salesforce, Microsoft, IBM, NetSuite, 3Tera, Rackspace, Joyent and others, such as AT&T, HP, Cisco, SAP, Red Hat and Verizon. IBM, for example, has recently invested billions in data centers in London, Sydney, Hong Kong and elsewhere.<sup>5</sup>

Because U.S. companies are so well-positioned in the worldwide high-tech market, they also have a lot to lose from foreign retaliation. Foreign citizens would view the transfer of their information from U.S. high-tech companies to the U.S. government as an invasion of personal privacy. Similarly, foreign businesses and governments would see the transfer to the U.S. government as a form of corporate and state espionage. At the very least, consumers and businesses would lose confidence in U.S. companies to protect their information.

Foreign leaders too will also be concerned about how this affects their citizens and businesses, as well as protecting the privacy of its leaders and secrecy of government information. This is particularly true in light of the recent NSA spying on foreign government leaders. In fact, foreign government leaders are already thinking twice before using U.S. technology products and services, such as email and cloud computing services. For protectionist countries, the attempt to usurp privacy laws provides an excuse to use only domestic servers, apps and communications services. The various privacy and legal issues have

---

<sup>4</sup> Ibid. Also see, Mike W. Thomas, "Could Spending Expected to Triple by 2017," *Alamo City Beat*, February 14, 2014, citing IHS estimates, see <http://www.bizjournals.com/sanantonio/blog/2014/02/cloud-spending-expected-to-triple-by-2017.html>.

<sup>5</sup> Claire Cain Miller, "Revelations of N.S. A. Spring Cost U.S. Tech Companies," *The New York Times*, March 21, 2014.

led some countries to be concerned about U.S. dominance in the high-tech sector, and has bolstered a growing anti-American sentiment:

The backlash in Europe extends beyond Google. Taxi drivers from London to Madrid have demonstrated against Uber, the American ride-sharing company that was recently banned in Germany. Apple and Amazon are being investigated over their tax policies, and regulators are scrutinizing Facebook's proposed acquisition of WhatsApp, a messaging app.<sup>6</sup>

### **The Cost of Economic Sanctions**

The U.S. has 10% of the world's online users, but only 4.5% of the population.<sup>7</sup> Yet, the U.S. has nearly one-third of research and development investment in science and technology.<sup>8</sup> However, its worldwide presence in technology could be threatened by a backlash of anti-American sentiment, now fueled by the Microsoft lawsuit and the resulting concerns of privacy and espionage.

While the Information Technology and Innovation Foundation predicted a \$35 billion loss in cloud computing from an international backlash from privacy concerns, Forrester Research estimated the larger high-tech sector could suffer financial losses as high as \$180 billion or about a quarter of industry revenues.<sup>9</sup> Using the Bureau of Economic Analysis industry multipliers, that loss would be equivalent to losing more than 2 million U.S. jobs. That would increase the unemployment rate by from 6.1% to 7.6%. These losses would be devastating for American high-tech businesses and could spill into non-tech commerce as well.

---

<sup>6</sup> Danny Hakim, "Google is Target of European Backlash on U.S. Tech Dominance," *The New York Times*, September 8, 2014, [http://www.nytimes.com/2014/09/09/technology/google-is-target-of-european-backlash-on-us-tech-dominance.html?\\_r=0](http://www.nytimes.com/2014/09/09/technology/google-is-target-of-european-backlash-on-us-tech-dominance.html?_r=0).

<sup>7</sup> <http://www.internetworldstats.com/top20.htm>.

<sup>8</sup> Lydia DePillis, "The U.S. is Losing Market Share in Global Science and Technology," *Washington Post*, February 2014, <http://www.washingtonpost.com/blogs/wonkblog/wp/2014/02/06/the-u-s-is-losing-market-share-in-global-science-and-technology-dont-panic/>.

<sup>9</sup> James Staten, "The Cost of PRISM Will Be Larger Than ITIF Projects," Forrester, Blog, August 14, 2013. Also see, Claire Cain Miller, "Revelations of N.S. A. Spring Cost U.S. Tech Companies," *The New York Times*, March 21, 2014.

Indeed, losses to U.S. corporations are already starting to surface. Following the NSA spying revelation, there were reports that IBM, Microsoft, Cisco and other American Companies may have lost customers and were not invited to bid on multi-year international contracts. The latest threat by the DOJ to access records on foreign consumers and businesses, particularly if successful in the courts, will certainly fuel further sanctions.

The shunning of U.S. high-tech products and services by consumers, businesses and governments will be a major setback for U.S. companies working abroad. Because the U.S. is a world leader in technological services and products, the effects of complying with the DOJ request would significantly stunt U.S. sales abroad and encourage foreign countries to buy products and services from their domestic sources, including developing a balkanized Internet that keeps its citizens, businesses and government away from buying U.S. products, cloud services, software and applications. This would affect U.S. competitive abroad for decades to come.

### **U.S. Government Needs to Fix This Mess**

The DOJ's quest for personal information on an Irish citizen living abroad could open up a cascade of problems overseas -- conflicts with laws in other countries, customer losses, contract sanctions by foreign business and governments, retaliation, and balkanization of the Internet. A balkanized Internet will not support the rapid growth of high-tech trade and free exchange of ideas that we have enjoyed over the past 20 years. It will lead to a substantial financial impact on U.S. high-tech firms and lost jobs for workers. It would also produce long-term harm to U.S. competitiveness in the high-tech sector.

The quick and easy solution is for the full and immediate attention of Congress in its consideration of legislation just introduced by Senators Hatch, Coons and Heller – *The Law*

*Enforcement Access to Data Stored Abroad Act.*<sup>10</sup> This proposed legislation would address the issue by limiting the reach of warrants to U.S. citizens and companies, as well as keeping conformity with foreign treaties and laws. Congress needs to act before the negative economic consequences of the DOJ's actions cause irreparable harm to U.S. interests abroad. The legislative solution makes the U.S. keep its promises and respect its legal treaties with other countries, and that works to dispel any fears of spying or collection of personal information that our allies might have.

We need to take steps now to protect U.S. business interests abroad. To do otherwise could lead to devastating financial consequences on U.S. high-tech firms.

---

<sup>10</sup> The LEADs Act, as it has been referred to, is available online at [http://www.hatch.senate.gov/public/\\_cache/files/c708f95d-3a68-46c9-8cf4-54c94586eb18/LEADS%20Act%20section-by-section,%20September%2018,%202014.pdf](http://www.hatch.senate.gov/public/_cache/files/c708f95d-3a68-46c9-8cf4-54c94586eb18/LEADS%20Act%20section-by-section,%20September%2018,%202014.pdf).