New York judge upholds US efforts to seize emails from Microsoft

Thomas Gaist
4 August 2014

New York federal district court Judge Loretta Preska ruled Thursday that US government warrants are valid for data stored overseas, as long as the company storing the data is based inside the United States.

The case stemmed from a federal warrant issued in December 2013 demanding data from a user account connected with an unspecified criminal investigation. Microsoft refused to turn over the data, and was subsequently ordered by a federal judge to do so in April of 2014.

Judge Preska rejected Microsoft's appeal of the April ruling, holding that emails stored on the company's servers in Dublin, Ireland and, by implication, all data controlled by US corporations, can be seized through the issuing of federal warrants, regardless of the location of the servers on which the data is stored.

"It is a question of control, not a question of the location of that information," Preska ruled.

Microsoft argued that the US requires consent from the Irish government, and is barred from directly grabbing data solely on the basis of its own warrant. Microsoft claimed that the "stored communications provisions" contained in the Electronic Communications Privacy Act (ECPA) do not apply to data stored overseas.

Other major technology corporations have backed Microsoft its legal contest with the US government, described in the media as a "cloud era test case," including Apple, Cisco, Verizon, and AT&T.

"There is nothing more critical than protecting the privacy and information of every single AT&T customer—no matter the country in which they reside," said Wayne Watts, a top official at AT&T.

"That's why we're extremely disappointed with today's US District court decision in favor of the US government's extraterritorial search warrant," Watts said.

The protestations of the tech companies against US government surveillance and data seizure, billed as a major "pushback" by the companies and the corporate media, cannot be taken at face value.

In reality, all of the major telecommunications providers have close working relations with the US government and have actively facilitated mass transfers of data to its surveillance and security agencies. The opposition of the tech corporations to US government efforts to legalize international data seizures is essentially a public relations exercise.

The companies are concerned about further damage to their profit margins resulting from the unveiled subordination of their overseas servers to the will of the American state. According to estimates compiled by the Information Technology and Innovation Foundation, revenues from US-based cloud computing may decline by tens of billions of dollars in the years ahead under the impact of the Edward Snowden exposures. The German government has already moved to terminate its contract with Verizon because of the company's systematic transfer of data to the NSA.

As Microsoft wrote in documents submitted to the court this June, "Over the course of the past year, Microsoft and other US technology companies have faced growing mistrust and concern about their ability to protect the privacy of personal information located outside the United States. The Government's position in this case further erodes that trust, and will ultimately erode the leadership of US technology companies in the global market."

Of course, the US government already has access to virtually every piece of data being produced worldwide by Microsoft users. The emails sought by the US in the Microsoft case could be acquired through a number of

existing warrantless surveillance and cyber-warfare programs.

As proven in documents leaked by Snowden, Microsoft has gone to great lengths to insure unfettered access to user data by the NSA. Microsoft has collaborated with the NSA's PRISM program since 2007, providing the agency with direct, unwarranted access to data generated by hundreds of millions of users of the company's cloud storage service, SkyDrive, and assisting NSA efforts to penetrate the company's own encryption systems.

Why then should the government bother waging such a high-profile legal battle? The US claims against Microsoft serve a political aim. The US is asserting unilateral jurisdiction over all data stored on servers around the globe, thereby legitimizing and expanding international surveillance practices which have, up to now, been carried out on a covert basis.