Patriot Act can "obtain" data in Europe, researchers say

LONDON European data stored in the "cloud" could be acquired and inspected by U.S. law enforcement and intelligence agencies, despite Europe's strong data protection laws, university researchers have suggested.

The research paper, titled "Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act," written by legal experts at the University of Amsterdam's Institute for Information Law, support previous reports that the anti-terror Patriot Act could be theoretically used by U.S. law enforcement to bypass strict European privacy laws to acquire citizen data within the European Union.

The Patriot Act, signed into law in 2001, granted some new powers to U.S. authorities, but it was mainly a "framework law" that amended and strengthened a variety of older laws, such as the Foreign Intelligence Services Act (FISA) and the Electronic Communications Privacy Act (ECPA).

"Most cloud providers, and certainly the market leaders, fall within the U.S. jurisdiction either because they are U.S. companies or conduct systematic business in the U.S.," Axel Arnbak, one of the authors of the research paper, told CBS News.

"In particular, the Foreign Intelligence Surveillance Amendments (FISA) Act makes it easy for U.S. authorities to circumvent local government institutions and mandate di-

Play ***Video***

Obama signs extension of Patriot Act

rect and easy access to cloud data belonging to non-Americans living outside the U.S., with little or no transparency obligations for such practices -- not even the number of actual requests."

This holds true for requests targeted at non-U.S. individuals and for entire business records, he added.

Dutch vice-chair of the European Parliament's civil liberties committee Sophie in 't Veld welcomed the research, adding that it "provided further evidence" to support the theory.

She told CBS News, however, that the European Commission's proposals for new data protection rules will not solve the potential conflicts posed by third country law and the lengthy period of time in which EU laws become ratified, "would not be a reason to let the situation be for several years to come."

Information security, privacy and data protection lawyer Bryan Cunningham, who worked under both democratic and republican administrations, most recently as deputy legal advisor to former U.S. National Security Advisor Condoleezza Rice under President George W. Bush, told CBS News that this "important report" should "help correct a widespread post-9/11 misconception," that the Patriot Act and related legislation, "provided vast new powers for the U.S. government to gain access to sensitive communications and data of non-U.S. persons."

The research resurfaces questions about the security and sovereignty of citizen and government data in an ever-connected global and borderless online world. It also supports a ZDNET report that European data protection rules do not protect EU citizens' data against extra-territorial third country law, such as that of the United States.

Months after the research was published, Microsoft U.K. managing director Gordon Frazer was the first to publicly admit that the software giant could not guarantee that European citizen data stored in EU-based data centers would not leave the European Union under any circumstances, including under a Patriot Act request.

"Neither can any other company," Frazer noted.

Frazer's disclosure triggered outrage among politicians in the European Parliament. Subsequently a number of European member state governments began to question their own cloud service provisions, and in some cases banned U.S. providers from offering IT and computing services in their countries.

U.K.-based defense giant BAE Systems in the past year reneged on plans to adopt Microsoft's cloud-based services, citing fears that critical national defense secrets could land in U.S. hands.

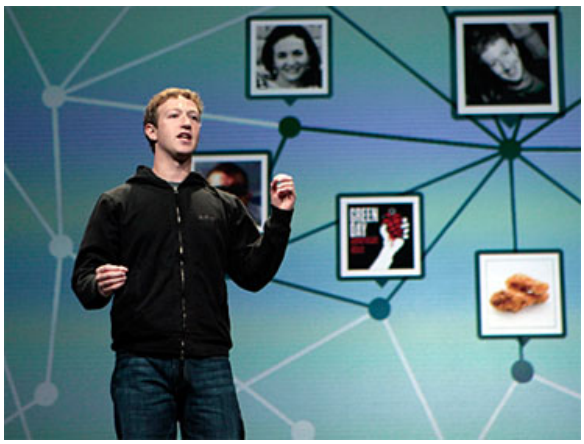
The Dutch government is also investigating a potential conflict with third country law in regards to personal citizen passport data. Dutch social-liberal party D66 raised questions in the country's parliament after suspicions arose that U.S. authorities could potentially access Dutch fingerprint and facial scans for passports because the North Holland-based company Morpho is owned by parent company Safran, which conducts systematic business in the U.S."

U.S. jurisdiction "extends to companies"

Cloud computing is the storing of documents, photos, music and files online. Governments, in possession of citizen data along with their own national security secrets, are increasingly utilizing cloud services for internal government communications, hosting documents and enabling the sharing of vast amounts of data between government departments.

Companies, schools and universities that wish to keep their data in their home jurisdiction -- governments, most of all -- the cloud poses a new set of risks.

Because most major cloud providers, such as Apple, Amazon, Google and Microsoft, are based in the U.S., the study was focused on the provisions under U.S. law, particularly in reference to the Patriot Act, signed in 2001, and the Foreign Surveillance Intelligence Act (FISA), originally signed into law in 1978 and last amended in 2008 by Congress.



Facebook is, basically, a giant cloud-based service, that can store your photos, videos, and other content, which is available from almost any device in the world.

/ **AP PHOTO/TOBY TALBOT**

The researchers explain that businesses, schools and universities located outside the United States -- including foreign governments -- which use cloud services offered by a company that conducts business in the U.S., could be forced by U.S. law enforcement to transfer data to U.S. territory for inspection by law enforcement agencies.

"In the U.S. legal framework, there is a legal doctrine called 'extra-territorial jurisdiction'. This implies that cloud providers operating

anywhere in the EU, or anywhere in the world for that matter, have to comply with data requests from U.S. authorities as soon as they fall under U.S. laws," said Arnbak.

"These laws, including the Patriot Act, apply as soon as a cloud service conducts systematic business in the United States. It's a widely held misconception that data actually has to be stored on servers physically located in the U.S."

If they are forced to hand over EU-stored data back to the U.S., the company could be found in breach of EU law, even if is covered by both EU and U.S. legal jurisdictions.

"The key criterion in this respect is whether the cloud provider conducts systematic business in the United States, for example because it is based there or is a subsidiary of a U.S.-based company that controls the data in question," the researchers write.

Because non-U.S. residents are not protected from unwarranted searches under the Fourth Amendment, the researchers warn that this "gives the U.S. government entities concerned the statutory power to gather data on a large scale about non-U.S. citizens located abroad. And, legal protection under specific U.S. laws applies primarily to U.S. citizens and residents."

However, under FISA -- amended by the Patriot Act in October 2001, just a month after the September 11 terrorist attacks -- foreigners were not the only group immune to unwarranted searches, the Fourth Amendment notwithstanding.

"The Bush administration had intercepted the communications of Americans without obtaining a judicial warrant. The New York Times had carried reports on this from late 2005," the researchers write.

The Patriot Act also added powers to FISA which, "enables the FBI to request access to business records for an investigation into espionage and terrorism involving both U.S. and non-U.S. persons."

However, while the researchers warn that U.S. law extends beyond the reach of its borders, figures relating to requests do not exist in the public domain.

- CNET: Patriot Act renewed despite warnings of 'secret' law
- This Internet provider pledges to put your privacy first. Always

The common misconception, according to the researchers, is that FISA gives the U.S. "unrestricted" or "unprecedented" access to data outside the country. FISA warrants

do go through a "special court known as the Foreign Intelligence Surveillance Court (FISC)." The role of the court is to, "review the acquisition of intelligence information in this way if U.S. government entities require the assistance of electronic communication service providers for this purpose."

This keeps highly sensitive requests for foreign data, under the premise of keeping terrorism-scale investigations secret, out of the public eye. Because FISA courts hold national security secrets and details of ongoing terrorism investigations, the researchers say the data can't and shouldn't be published.

"Given the nature of intelligence work, it is not possible to gain insight into actual requests for information by the U.S. authorities, other than a description of the general legal framework," the researchers write.

EU citizens "at risk" from FISA, Patriot Act

While most Americans are aware of the Patriot Act and its wide-ranging provisions for domestic security, its role outside the U.S. border remains widely unknown.

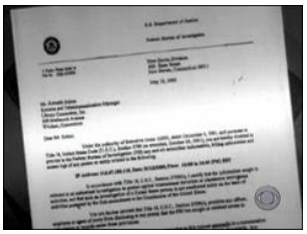
While the researchers focused their efforts on the data protection of cloud users in higher education in the Netherlands, in speaking to CBS News, Arnbak warned that the concern over the ability of third countries accessing data stored in the European Union was not limited to the Netherlands, but that it "certainly" extends to the 27 member state bloc, and even outside the European Union.

"The risk of data access by U.S. authorities to cloud data is realistic, and should form an integral part in any decision making process to move data into the cloud," he said.

Because the Netherlands is a member of the European Union, the country's data protection laws originally stemmed from a wider directive from the European Commission.

Ratified in 1995, the EU Data Protection Directive must have been subsequently implemented into the legal systems of all member states by 1998. Therefore, every EU member state has the same foundation framework for data protection and privacy as each other, giving member state governments to expand upon the base principles and allowing data to freely flow across member states' borders, just as EU citizens have the right to do.

"This concerns anyone with an interest in autonomy and control over access to data -- governments, businesses, non-profits and consumers alike. That's why the current de-



Play ***Video***

Audit Raps FBI On Privacy

bate on electronic heath records in The Netherlands is both fascinating and very serious. It appears that nobody has looked into this risk, before investing millions of taxpayers money to build these systems," Arnbak said.

He noted that businesses and governments alike, despite the additional costs, should consider in-house solutions instead of moving to the cloud. "If data is processed in-house, institutions will at the very least know of such investigations at an early stage."

Cunningham says, "There remains no credible way -- short, perhaps, of end-to-end encryption with the data provider holding the only key -- to assure confidentiality and security for cloud-stored data, whether stored in the United States or elsewhere."

"Governments and institutions seeking such privacy and security protections should, at least for now, stick to storing their own data or, perhaps, implementing national cloud solutions with robust privacy and security protections."

Because the U.S. government has "ample possibilities to request data from foreign (in this case Dutch) users of the cloud," the researchers claim, "it grants [authorities] to retrieve information on a large scale, including access to complete data sets."

"In other words, these agencies may obtain information not only about a student who could pose a threat to U.S. national security but also about a student who makes an appointment in good faith through email with a person suspected by U.S. authorities of drug trafficking," the researchers assert.

But this also extends outside the Netherlands to countries both in and outside the European Union. "From the U.S. legal perspective, Dutch users of cloud-based computing services therefore enjoy the same degree of [U.S.] constitutional protection as North Koreans," the study says.

However, the U.S. is not alone with laws reminiscent of FISA or the Patriot Act. The researchers note that such wide-ranging provisions able to access cloud-stored data outside of their respective jurisdictions are not limited to the U.S. And continue to say, "Other nation states, including the Netherlands, have comparable provisions in place for access to data in the context of law enforcement and national security."

For instance, the report notes the Dutch Intelligence and Security Services Act, which give the Dutch security and intelligence services, "the power to process the personal

data of a wide range of persons." One of the sections of the law specifically carries FISA-like provisions in the Netherlands, which, "authorizes them to carry out, using a technical aid, targeted tapping, reception, recording and interception of any form of conversation, telecommunication or data transfer by means of an automated activity, irrespective of where this takes place."

Similarly, the Canadian Anti-Terrorism Act "replicates" much of the provisions in the U.S.' Patriot Act. Ontario's Information and Privacy Commissioner Ann Cavoukian said in a recent report that the Act's provisions are part of the normal data-sharing process between governments.

"You can outsource services, but you cannot outsource accountability," Cavoukian says.

"Legal provisions regulating data access for intelligence and law enforcement purposes will exist in all democracies," Arnbak says.

Cunningham warns that large, multinational, private cloud companies could pose a greater risk to private and sensitive citizen data than governments.

"Many intelligence services around the world, particularly in non-democratic countries, have no effective legal restrictions whatsoever, and are aggressively collecting massive amounts of sensitive personal, government, and commercially valuable information around the world," Cunningham says.

"Particularly with the rise of large, lightly-regulated cloud data storage providers, private, multinational companies actually may have more access to sensitive, personal data than national governments." Cunningham continues to say, such firms "assert far more authority to combine and data-mine such data for their own purposes than would the government be permitted under U.S. law."

"And, whether or not such companies would intend to misuse such data, they are far from immune from ill-motivated insiders and external hacking activities, by individuals, criminal groups, and foreign governments."

As a result, many countries can also theoretically acquire data stored by companies in another country without a mutual legal assistance request -- used by governments to request help in obtaining evidence from another jurisdiction to assist in investigations in another -- if the company is required by that country's domestic law to assist, in spite of any protection offered by a third country's legal system.

This could include cloud-stored medical data, financial information provided by banks, and business documents or corporate secrets, all the way down to an ordinary user's cloud-stored iTunes music collection or the cloud-stored photos taken on a recent vacation.

Because the U.S. is home to the global powerhouses that run major cloud services -- not limited to Apple, Amazon, Google and Microsoft -- the research increases the scope of relevance to cloud users. Conversely, the report notes that the company may not have to be headquartered in the U.S. to be supposedly susceptible to a data access request.

- CNET: FBI: We need wiretap-ready Web sites - now
- Supreme Court closes door on warrantless eavesdropping suit

"If a company has a subsidiary or branch in the United States, it may be assumed that such jurisdiction exists, but jurisdiction may also exist in other more complex cases," the researchers assert.

Authorities, however, are more likely to be interested in the electronic communications between two or more persons, rather than a citizen's recent holiday photos.

In the case of cloud-stored email, which many businesses, schools, universities and ordinary citizens use, this can be hosted by an EU-based subsidiary of a U.S.-based parent company. U.S. residents enjoy not only Fourth Amendment protection from unwarranted searches, but also additional protection from the Electronic Communications Privacy Act (ECPA) and the Stored Communications Act (SCA), which regulates the U.S. government's access to electronically stored data, such as email, in criminal investigations.

One of the strongest legal protections, the researchers note, under the SCA is the provision that requires U.S. authorities to request a search warrant from a judge, based on grounds of reasonable suspicion, if email is less than 180 days old. This law recently came to light after the recent resignation of Gen. David Petraeus, the former direc-

Play ***Video***

Petraeus scandal developments

tor of the Central Intelligence Agency. A warrant from only a federal prosecutor is required to acquire emails that are older than six months.

However, if U.S. federal authorities requested foreign citizen data, they would not receive protection under the Fourth Amendment, nor would the receive any protection from the ECPA or the SCA, because, "the position remains that if a person whose records have been requested is not a U.S. person and is not located in the United States, he cannot invoke the protection of the Fourth Amendment," the research states.

The academics warn that, while in some cases, contracts can be offered to cloud customers; these do not override judicial requests by third countries. "The possibility that foreign governments request information is a risk that cannot be eliminated by contractual guarantees."

Did EU laws ever protect against third country snooping?

The EU's Data Protection Directive 1995 states that EU personal data may only be transferred outside the 27 member state bloc if that country provides guarantees that the data will be given an adequate level of protection.

Data stored in the European Union freely flows to the U.S. so long as the company or government department receiving the data adheres to the EU's Safe Harbor Principles, which were set up between the U.S. government and the European Union after the EU data and privacy laws were first ratified in 1995. The rules help U.S. recipients of EU observe basis EU data protection rules in order to prevent data loss or accidental data disclosure by U.S. companies receiving EU data.

However, the Patriot Act, signed into law in 2001, granted some new powers to U.S. authorities, but it was mainly a 'framework law' that amended and strengthened a variety of older laws, such as FISA and ECPA. The 2001 Act has since been amended numerous times to extend its powers. FISA, which provides authorities to acquire cloud-stored data in foreign countries and jurisdictions, was first signed into law in 1978, and has also been amended numerous times to keep up to date with current technological trends.

While suggesting that the Patriot Act's bypassed the protection of European data by the EU Data Protection Directive, allowing data to be potentially transferred outside

the EU via a U.S.-based company, one former U.S. government lawyer noted that the Patriot Act did not substantially change how the U.S. government acquires data for intelligence purposes.

ZDNET's report suggests that the Patriot Act's "negated" the protection of European data by the EU Data Protection Directive, allowing data to be potentially transferred outside the EU via a U.S.-based company. Politicians in the European Union raised questions over laws that may affect their own nation's legal system.

- ZDNet: USA PATRIOT Act series
- U.S. warrantless surveillance memos remain sealed

Cunningham told CBS News that with appropriate judicial or other government procedures, "U.S. law enforcement and security authorities remain, as they were before the Patriot Act, able to lawfully collect both the substance of electronic communications and telephone toll, e-mail, and other business records, both of U.S. persons and those of other countries, without resort to mutual legal assistance or other international agreements and procedures."

"This is particularly true when such data is held by companies physically located in, or with substantial business connections to, the United States," he continues.

U.K., Netherlands raise concerns over cloud legal issues

There are already existing agreements and data-sharing arrangements between EU member states and non-member states, such as the U.S., the issues relating FISA and the Patriot Act notwithstanding. Without it, most Europeans would not even be allowed to step on an airplane bound for the U.S.

Mutual legal assistance (MLA) agreements exist between various nations, which conform with EU data protection and privacy laws, in order assist nations outside both within and outside the 27 member state bloc in criminal investigations. For instance, the U.S., Australia, or any other country with an MLA agreement with the Netherlands can request data on a Dutch citizen data, just as the Netherlands can in return.

"If U.S. government agencies have no jurisdiction over an entity operating in the Netherlands, they may submit a request for mutual assistance under such agreements," the researchers state.

"But in the borderless cloud, in which activities are in the U.S., there is "no clear obligation under U.S. law for the U.S. government to rely on such agreements when seek-

Apple's cloud services allows you to access your documents from any Apple device or computer with an Internet connection.

/ **Donald Bell/CNET**

ing access to data on non-U.S. persons."

Also, passenger name record (PNR) data sharing agreements between the EU and Australia, Canada and the U.S., not only allow citizens to travel between those countries, but also help those authorities fight transnational crime.

PNR data includes personal and sensitive citizen data, such as their name, gender, date of birth and nationality. It can also include "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or concerning the health or sex life," according to the European Commission, but notes that PNR data "rarely contain sensitive data of this kind."