A Hogan Lovells White Paper

Individual Rights to Challenge Government Access to Data in the Cloud

A comparison of the protections for individuals in the United States, Australia, France, Germany, and the United Kingdom

by

Christopher Wolf, Bret Cohen, and James Denvil*

September 23, 2013

All of the countries surveyed for this White Paper provide citizens and non-citizens alike with the ability to challenge government access to data they store with a Cloud service provider, as well as remedies if they suffer harm from unlawful government access. The right of redress, however, appears strongest in the United States.

The use of Internet services in the "Cloud" that allow individuals to upload, store, and access data on remote servers is growing. Storage and management of email, documents, and photos in the Cloud is commonplace. But with the growth of Cloud computing by individuals is a concern over government access to data residing with Cloud providers. This White Paper examines what rights and remedies individuals have if their data are disclosed to a government agency.

The focus of this White Paper is on the ability of individuals to challenge government access to their data in the cloud, and the decisions governments make based on that data. While there is current controversy over national security access to data held by Cloud providers, those policy challenges – and the ability to challenge government national security surveillance in each of the in-scope countries – are beyond the scope of this White Paper.[1] Still, with respect to the United States, we do note remedies available to individuals when the government conducts illegal national security surveillance.

As detailed in the 2012 Hogan Lovells White Paper "A Global Reality: Governmental Access to Data in the Cloud" ("Governmental Access White Paper"),[2] all countries give the government the authority to require a Cloud service provider to disclose customer data when conducting lawful government investigations. This prompts the following questions regarding an individual's rights when a government actually does access an individual's data in the Cloud:

1. Can an individual challenge the government's access to data in the Cloud (even if not a citizen of that country)?

2. If an individual is placed on a security watchlist (such as a no-fly list) as a result of the government's unlawful access to data stored in the Cloud, what rights does the individual have to challenge that action?

To answer these questions, we examined the laws of the United States, Australia, France, Germany, and the United Kingdom.

Summary

As summarized in our Governmental Access White Paper, governments face limits on access to data from a Cloud service provider, and the United States establishes some limits that many other countries do not establish. For example, the United States bars a Cloud service provider from voluntarily disclosing customer data to the government in response to an informal request, instead requiring such requests be made through legal process.

All of the countries surveyed for this White Paper provide citizens and non-citizens alike with the ability to challenge government access to data they store with a Cloud service provider during the course of typical criminal and administrative investigations, as well as remedies if they suffer harm from unlawful government access.

The right of redress, however, appears strongest in the United States, as it is the only country among those surveyed that provides for all of the following: 1) minimum

* Mr. Wolf is a partner and Director of the Privacy and Information Management practice of Hogan Lovells US LLP, where Messrs. Cohen and Denvil are associates. Special thanks to Hogan Lovells colleagues Winston Maxwell, Lionel de Souza, and Sarah Taieb (France); Stefan Schuppert, Martin Pflüger, and Maira Baderschneider (Germany); and Mac Macmillan, Matt Sharkey, and Ed Southall (UK), and to Tim Brookes, Susan Goodman, and Tanvi Mehta (Australia), for their assistance in the study of the laws around the world.

[1] For a comparative analysis of different countries' national security surveillance laws, see Winston Maxwell & Christopher Wolf, *A Sober Look at National Security Access to Data in the Cloud* (2013), *available at* http://hldataprotection.com/2013/05/articles/international-eu-privacy/white-paper-cloud-national-security.

[2] Winston Maxwell & Christopher Wolf, *A Global Reality: Governmental Access to Data in the Cloud* (2012), *available at* http://hldataprotection.com/2012/05/articles/international-eu-privacy/hogan-lovells-white-paper-on-governmental-access-to-data-in-the-cloud-debunks-faulty-assumption-that-us-access-is-unique.

statutory damages for the government's unlawful access to Cloud data; 2) the ability to sue government officials in their individual capacity for unlawfully accessing Cloud data; and 3) the ability to challenge and appeal decisions regarding placement on a no-fly list. The United States is also the only country that gives courts the authority to require a government agency to initiate a disciplinary proceeding against a government employee based on a suspicion that the employee unlawfully accessed Cloud data.

United States

Can an individual challenge the U.S. government's access to data in the Cloud (even if not a U.S. citizen)?

Yes. U.S. federal law protects U.S. citizens and non-citizens alike when the government seeks information stored in the Cloud during the course of typical criminal and administrative investigations.

In most circumstances, government access to data stored with a Cloud service provider is regulated under the Electronic Communications Privacy Act ("ECPA"). ECPA firmly requires the government to use specified legal mechanisms (such as search warrants, special ECPA court orders, and valid subpoenas[3]) when it wishes to obtain customer data from a Cloud service provider. (As noted above, U.S. Cloud providers may not voluntarily disclose Cloud data, even when the government asks for it.)

Whatever method the government uses, **ECPA requires judicial authorization or customer notice.** If the government accesses data in violation of ECPA, the statute provides specific remedies. Individuals may recover the greater of $10,000 or their actual damages, plus reasonable litigation costs if they establish that the U.S. government willfully violated the act. And if a court or government authority determines that there are "serious questions" about whether a federal employee has willfully or intentionally violated ECPA, the responsible agency must promptly hold proceedings to determine if disciplinary actions are warranted. If the agency determines that discipline is not warranted, the Inspector General with jurisdiction over the agency must be provided with reasons for that determination.

U.S. law also allows individuals whose data have been accessed in violation of ECPA to recover damages directly from responsible federal officials in their personal capacity, municipal governments, and state or local officials. Because ECPA's statutory damages provision does not require proof of actual harm, individuals may recover a minimum of $10,000 from the government based solely on the government's unlawful access to stored data. When suing individuals, the minimum damages award is $1,000, plus reasonable attorney's fees and litigation costs.

Who counts as an "aggrieved person" under ECPA? ECPA protects "persons." U.S. courts long have held that "person" is a universal term referring to *all* individuals sufficiently connected to the United States, including foreign nationals. When Constitutional provisions or federal laws extend rights to persons, **U.S. courts hold that those rights belong to foreign nationals** as well as U.S. citizens. A high-level U.S. appellate court (one level below the Supreme Court) specifically has held that ECPA's protections extend to non-U.S. citizens who store data in U.S.-based Cloud servers.[4] No appellate court has challenged that ruling.

Therefore, whether you are a U.S. citizen or a foreign national, ECPA allows you to challenge the U.S. government's access to information that you have stored on the Cloud.

How would you know that the government has accessed your data? As mentioned above, under ECPA **the government must obtain judicial authorization to obtain customer data or it must notify affected customers.** If the government demonstrates that prior notice would endanger a person's physical safety or compromise the investigation, notice may be delayed.

The U.S. Freedom of Information Act ("FOIA") also provides an important check against secretive government actions. FOIA allows all people, "regardless of citizenship, to gain access to records held by [U.S.] government agencies."[5] Individuals can appeal to courts to *compel* executive agencies that refuse or fail to comply with FOIA requests in a timely manner. FOIA does allow the government to withhold certain categories of information under specific narrowly applied exemptions. But individuals can challenge the validity of an agency's application of those exemptions all the way to the U.S. Supreme Court.

If an individual is placed on a security watchlist (such as a no-fly list) as a result of the government's unlawful access to data stored in the Cloud, what rights does the individual have to challenge that action?

Under the Fifth Amendment to the U.S. Constitution, the government may not deprive a person of a liberty or property interest without due process of law. **And because U.S. courts interpret "person" to be a universal term that includes foreign nationals, the U.S. government must provide Constitutional due process to foreign**

[3] More information about these legal mechanisms is available in our Governmental Access White Paper. Although outside of the scope of this White Paper, in that paper we also detail how National Security Letters ("NSLs") are limited to non-content identifying information and that the "gag order" options that may be exercised when the government serves NSLs are subject to judicial challenge.

[4] *Suzlon Energy Ltd. v. Microsoft Corp.*, 671 F.3d 726 (9th Cir. 2011).

[5] Mary Ellen Callahan, Chief Privacy Officer, U.S. Dep't of Homeland Security, *Finding Relief for Privacy Infringements in the New World* (2009), *available at* https://dhs.gov/xlibrary/assets/privacy/privacy_us_finding_relief_privacy_infringements.pdf.

nationals living outside the United States when it acts against such individuals inside U.S. territory. The U.S. Supreme Court has stated: "To be sure, aliens as well as citizens are entitled to the protection of the Fifth Amendment."[6]

What does that mean exactly? The government cannot deprive an individual of property or liberty without meeting certain procedural requirements. Criminal trials must provide due process, and legal challenges are available to address the government's use of data obtained illegally (e.g., in violation of ECPA). **Foreign citizens have similar rights when challenging administrative decisions, such as removal proceedings under immigration laws.**

For those concerned about watchlist or travel issues, foreign nationals have an avenue for redress through the U.S. Department of Homeland Security ("DHS"), including its Privacy Office. The Department's Traveler Redress Inquiry Program[7] allows individuals to register inquiries or concerns regarding difficulties they experience during travel. If an individual is not satisfied with DHS's final determination of his or her issue, the individual may request an appeal in federal court. Essentially, if someone thinks the government has made an adverse decision based on information the government obtained unlawfully from a Cloud provider, there are ways to mount an administrative challenge and bring that challenge before a judge.

In short, U.S. law restricts government access to customer data held on Cloud servers in the United States, even if the data belongs to foreign nationals living abroad. And foreign nationals have a variety of avenues for redress should they feel that their rights have been violated by the government.

A note about remedies for illegal national security access

While ECPA regulates government access to data stored with a Cloud service provider during the course of typical criminal and administrative investigations, a separate legal regime, the Foreign Intelligence Surveillance Act ("FISA"), governs how law enforcement agencies can obtain information about persons during the course of certain investigations related to national security or foreign terrorism.[8] While redress rights under FISA and other countries' national security surveillance laws are not the focus of this White Paper, we note that individuals have similar redress rights under FISA as they do under ECPA if their data are acquired unlawfully. Specifically, they are entitled to recovery against the United States for the greater of $10,000 or actual damages plus reasonable litigation costs, responsible government authorities are required to promptly hold disciplinary proceedings if there are "serious questions" about whether a federal employee has willfully or intentionally violated FISA (and can be ordered to do so by a court), and individuals (except for agents of a foreign power) whose data have been accessed in violation of FISA may sue responsible government officials personally for a minimum of $1,000 or $100 per day for each day of the violation, whichever is greater, plus reasonable attorney's fees and litigation costs. And before any evidence gathered under FISA can be used in a criminal trial, the government must first notify the defendant, who then can move to suppress the evidence on the grounds that either the information was unlawfully acquired or the surveillance was not conducted in conformity with the order authorizing or approving it.

Australia

Can an individual challenge the Australian government's access to data in the Cloud (even if not an Australian citizen)?

Yes. If the government seizes Cloud data, the warrant or notice authorizing the seizure may be challenged in the courts by all affected individuals, including foreign nationals, who demonstrate that the government has interfered with their private rights, or who show that they have a special interest in the issuance of the warrant (as may be the case where data about an individual is being held by a Cloud service provider). When reviewing the decision to issue a warrant, Australian courts examine the legislation under which access to the data was granted and consider whether the required threshold for granting access was met. If the reviewing court finds that the search warrant was issued unlawfully, the court will declare the warrant to be invalid.

Besides simply challenging warrants, individuals may also recover damages for unlawful access. The Telecommunications (Interception and Access) Act 1979 gives individuals the right to sue government agencies that have accessed certain stored communications in violation of the Act. Unlike ECPA, however, the Act does not provide for minimum statutory damages. Individuals may also bring an action against the government or government officials for the tort of misfeasance in public office. This tort, however, is notoriously difficult to prove; to succeed, plaintiffs must prove that the unlawful access caused harm or loss and that government officials acted with knowledge of or intent to cause the harm suffered. Mere access would not be sufficient to establish the right to damages.

Unlike in the United States, there is no statutory authority in Australia for courts to order government agencies to initiate proceedings to determine whether disciplinary actions are warranted. The Office of the Australian Information Commissioner ("OAIC") does, however, have the authority to require an agency to change its policies and procedures and to require that the responsible individuals receive counseling when there is improper access to personal information.

---

[6] *United States v. Pink*, 315 U.S. 203, 228 (1942) (citing *Russian Volunteer Fleet v. United States*, 282 U.S. 481 (1931)).
[7] DHS, Traveler Redress Inquiry Program, http://dhs.gov/dhs-trip.
[8] *See generally* Winston Maxwell & Christopher Wolf, *A Sober Look at National Security Access to Data in the Cloud* (2013).

If an individual is placed on a security watchlist (such as a no-fly list) as a result of the government's unlawful access to data stored in the Cloud, what rights does the individual have to challenge that action?

Rather than a no-fly list, the Australian Department of Immigration and Citizenship ("DIAC") maintains a Movement Alert List ("MAL"). MAL contains information about non-citizens who are of concern to the Australian government, and the list is not available to the public. Individuals who believe that they may be included in MAL may file informal complaints with the DIAC. If the complaints are not addressed satisfactorily, individuals may escalate the complaints to the OAIC. There is no judicial review available for an individual to challenge his or her placement in MAL.

France

Can an individual challenge the French government's access to data in the Cloud (even if not a French citizen)?

Yes. All individuals, including foreign nationals, who become aware that the government has requested their data can challenge the validity of the request before the investigation appeals court (*Chambre de l'instruction*).

In evaluating an individual's challenge to a government data request, the court considers whether the requesting official had legal authority to issue the search request and whether proper search procedures were followed. The court will not invalidate the government's request for access if any irregularities found were minor or the individual bringing the challenge was not harmed.

Individuals also may sue the government for damages arising from unlawful access to data, but no law grants individuals the ability to recover mandatory minimum damages based solely on the fact that a government official unlawfully accessed their data. Regardless of whether the unlawful access took place in an administrative or criminal context, individuals must show that they suffered some tangible harm. And in administrative procedures, individuals must show that the responsible authority committed a very serious fault (*faute lourde*).

Government officials may be found liable in their individual capacity for unlawful access to data stored in the Cloud, but only if their actions are separable from their official professional activities and constitute serious misconduct (for example, if an official acts with a malevolent or wicked intention or accesses data for the official's personal use). Therefore, it is unlikely that an officer's intentional access of data during the course of an investigation, even if performed with knowledge that the access is unlawful, would suffice to establish personal liability. If liability were established, individuals would be able to recover only for damages suffered; there is no recovery for mere unlawful access.

French law does authorize the investigation appeals court, in its discretion, to order disciplinary measures against government officials.

If an individual is placed on a security watchlist (such as a no-fly list) as a result of the government's unlawful access to data stored in the Cloud, what rights does the individual have to challenge that action?

If individuals challenge their placement on a no-fly list, security watchlist, or a wanted persons file, they may request access to the data relating to them and petition to rectify or suppress any data that is inaccurate or was improperly included. Individuals may access no-fly lists, and other lists related to security and defense, by filing a request with the French data protection authority ("CNIL"). The CNIL transmits these requests to the public prosecutor, who then decides whether the requests are justified. If the public prosecutor refuses an individual's request to access or remove personal data from a list, the individual may appeal to the judge of liberties and detention. That judge's decisions are subject to appeal before the president of the investigation appeals court.

Germany

Can an individual challenge the German government's access to data in the Cloud (even if not a German citizen)?

Yes. All concerned parties with a legitimate interest (this might include individuals with personal information on the seized or searched servers), including foreign nationals, may challenge the warrant authorizing a search and seizure by filing a complaint with the issuing court. The court has discretion to suspend enforcement actions while reviewing the complaint and renders its decisions without holding a hearing. If the court decides that the complaint is well-founded, it can cancel the warrant. Individuals have no right to appeal the court's decision.

Law enforcement officials must conduct all searches and seizures of a Cloud provider's servers in accordance with the German Code of Criminal Procedure. Individuals may sue the government for unlawfully accessing data, but claims may not be brought against government officials themselves. To prevail against the government, individuals must show that 1) their rights were violated 2) by government officials acting 3) intentionally or negligently 4) in their official capacity 5) resulting in damages. To recover damages for the unlawful access, individuals must show that they have suffered measurable harm; there is no provision for mandatory minimum damages for unlawful access to Cloud data as there is in U.S. law.

If there is sufficient evidence to support the suspicion that an official has breached his or her duty, the official's supervisor must initiate disciplinary proceedings. But this decision is entirely in the discretion of the supervisory authority. The courts do not have authority to order agencies to initiate disciplinary proceedings, as is the case in the United States.

If an individual is placed on a security watchlist (such as a no-fly list) as a result of the government's unlawful access to data stored in the Cloud, what rights does the individual have to challenge that action?

When individuals are adversely affected by actions taken by German governmental authorities, they have the right to have those actions reviewed. If an authority places an individual on a no-fly list by issuing an administrative order or even by acting without a formal order, the affected individual may file an objection with the authority. If the authority does not provide redress, the individual may appeal before the administrative courts, asking for injunctive relief and for a decision on the merits. Administrative court decisions are subject to appeal.

United Kingdom

Can an individual challenge the UK government's access to data in the Cloud (even if not a UK citizen)?

Yes. Both citizens and non-citizens can lodge complaints about requests made under the Regulation of Investigatory Powers Act for traffic, usage, or subscriber data with the Investigatory Powers Tribunal ("Tribunal"). If the Tribunal finds that an individual's challenge is valid (i.e., that a warrant or authorization should not have been given or that there were procedural flaws), it may quash or cancel the warrant or authorization and order that the government destroy the data it obtained. Should the Tribunal deny an individual's challenge, there is no redress outside an appeal to the European Court of Human Rights. If the government obtains data under the Serious Organised Crime and Police Act 2005, the Police and Criminal Evidence Act 1984, or other more specific statutes that grant the police powers of search and seizure, affected individuals can appeal those searches through the court system.

The Tribunal has the power to award any compensation it deems appropriate to affected individuals. Historically, the Tribunal has been unlikely to award compensation where the complainant has not suffered any pecuniary loss. If Cloud data is accessed via a search and seizure warrant that is itself unlawful or that is executed unlawfully, affected individuals may file suit against the government under the Human Rights Act 1998. Alternatively, affected individuals may be able to file suit for trespass. In either case, damages will be assessed based on the individual's actual loss. There is no right of recovery for mere unlawful access, as is the case in the United States.

Individuals can also file suit against government officials. If data is accessed in breach of the codes of practice issued under the Police and Criminal Evidence Act 1984, the breach may constitute a civil tort. Intentionally accessing data stored on a computer without authority may constitute a breach of the statutory duty under the Computer Misuse Act 1990. Unlawful access may also constitute a trespass, breach of confidence, or misuse of private information. To recover damages under any of these causes of action, individuals would have to establish that they had suffered a loss. The mere unlawful access to data would not give individuals the right to recover damages.

United Kingdom laws do not give courts the authority to order government agencies to initiate disciplinary proceedings based on unlawful access to Cloud data.

If an individual is placed on a security watchlist (such as a no-fly list) as a result of the government's unlawful access to data stored in the Cloud, what rights does the individual have to challenge that action?

Individuals who suffer adverse administrative decisions based on the government's unlawful seizure of Cloud data, such as by being placed on a security watchlist or no-fly list, can challenge these decisions through judicial review. Before doing so, these individuals must submit a letter and attempt to resolve their issues through alternative dispute resolution. If that process is not successful and individuals wish to proceed with their claims, they must make an application for judicial review in the courts. If the courts view that there are grounds for judicial review, permission will be granted. Defendants have no right to appeal the courts' decisions.

GOVERNMENTAL AUTHORITIES' ACCESS TO DATA IN THE CLOUD AND INDIVIDUALS' RIGHT TO REDRESS: A COMPARISON

	May government require a Cloud provider to disclose customer data in the course of a government investigation?	May a Cloud provider voluntarily disclose customer data to the government in response to an informal request?	If a Cloud provider must disclose customer data to the government, must the customer be notified?	May non-citizens challenge government access to their data in the Cloud?	Can individuals recover mandatory minimum damages for unlawful access to Cloud data by the government absent a showing of harm?	Can individuals obtain damages from government officials in their individual capacity for unlawful access to Cloud data?	Can courts require the government to initiate a disciplinary proceeding against an employee for unlawful access to Cloud data?	May non-citizens seek judicial review of their placement on a security watchlist (e.g., no-fly list)?
Australia	Yes	Yes, except for personal data without a legal purpose	No	Yes	No, can only recover for actual harm	Yes, but can only recover for actual harm	No	No, only informal complaint to administrative body available
France	Yes	Yes, except for personal data without a legal purpose, electronic communications	No	Yes	No, can only recover for actual harm, and in an administrative context, must show a serious fault	Yes, but must show that the official acted maliciously and can only recover for actual harm	Yes	Yes
Germany	Yes	Yes, except for personal data without a legal purpose, electronic communications	Yes, except may withhold until disclosure no longer would compromise the investigation or in investigation of serious criminal offenses, national security, or terrorism	Yes	No, can only recover for actual harm	No	No	Yes
United Kingdom	Yes	Yes, except for personal data without a legal purpose	No	Yes	No, can only recover for actual harm	Yes, but can only recover for actual harm	No	Yes
United States	Yes	No, data must be requested through legal process	Yes, for content data, except when the government obtains a search warrant or unless disclosure would compromise the investigation	Yes	Yes, $10,000	Yes, minimum damages would be $1,000	Yes	Yes