Executive Summary

The US government has extensive “legal intercept” regulations that require US and foreign IT operators to allow US agencies to penetrate their operations. Other governments doubtless have parallel legal intercept regulations of their own, although how extensive these might be is not publicly known. To prevent discrimination against themselves, many US IT companies and suppliers are arguing for a robust, principled, transparent framework to govern lawful requests for data across jurisdictions. Without such a framework, the worldwide telecommunications market could continue to segment as governments and private buyers in foreign countries attempt to avoid US government surveillance measures.

This paper summarizes the major US legal intercept programs to tap into the databases and IT networks of US firms and foreign firms based in the United States and to limit or prevent foreign firms from conducting reciprocal surveillance. How do these surveillance and antisurveillance programs work? To whom do they apply? To what extent do they apply to the overseas operations of US firms? To what extent do they apply to foreign firms when they enter the US market?

These programs can be gathered into four clusters:

1. US government electronic surveillance under the Patriot Act, the Foreign Intelligence Surveillance (FISA) Court, and the FISA Amendments Act. These acts specify what the government can surveil during an investigation, and the FISA Court hears requests from the government to conduct such surveillance.

2. The Federal Communications Commission, international licenses, and “Team Telecom.” These control the processes by which telecommunications providers that have any foreign ownership are authorized to offer services between the US and foreign countries.

3. The Communications Assistance for Law Enforcement Act (CALEA) and the requirement to design penetration-friendly hardware and software. CALEA requirements apply to all foreign telecom service providers or switching equipment suppliers operating in the US and govern how they must design hardware and software to permit US government surveillance.

4. The Committee on Foreign Investment in the United States (CFIUS). This committee is not a legal-intercept program, but it interacts with US legal-intercept programs to review foreign acquisitions. CFIUS may also help to prevent surveillance activities by foreign firms that acquire US companies.

A mutual legal assistance treaty to prevent the balkanization of IT markets would need to cover sensitive issues surrounding legal intercept processes in each signatory nation and would require cooperation and transparency from nations around the world. This analysis of current US practices will help contribute to the formulation of such a framework.

However, some companies are choosing to counter US government surveillance regulations by creating controls on their devices so that nobody but the device’s owner can access its content. Apple and Google have already taken such steps, and their major competitors around the world are likely to follow suit. Such actions would limit the ability of law enforcement authorities to conduct surveillance on criminal and terrorist activity, even when they have a warrant.
US Government Surveillance Regulations for
IT Company Networks: Toward a Global Framework

The Trans-Pacific Partnership, the Trans-Atlantic Trade and Investment Agreement, the US-China Bilateral Investment Treaty, and other investment agreements contain important proposals to introduce greater transparency into national security investigations of foreign acquisitions by the Committee on Foreign Investment in the United States (CFIUS) and counterpart agencies in other countries. But, as this paper will make clear, national security regulations that govern foreign acquisitions are only a small part of the mandates to which information technology, telecommunications, and other electronics companies are subjected in the United States and abroad.

This paper summarizes the major US “legal intercept” programs to tap into the databases and IT networks of US firms and foreign firms based in the United States and to limit or prevent foreign firms from conducting reciprocal surveillance in the United States. These programs can be gathered into four clusters:

1. US government electronic surveillance under Sections 215 (the “business records” provision) and 216 (the “access to online activity” provision) of the Patriot Act, the Foreign Intelligence Surveillance (FISA) Court, and Section 702 of the FISA Amendments Act;

2. The Federal Communications Commission (FCC), licenses under Section 214 of the Communications Act of 1934, and “Team Telecom”;

3. The Communications Assistance for Law Enforcement Act (CALEA) and the requirement to design penetration-friendly hardware and software; and

4. The Committee on Foreign Investment in the United States (CFIUS).

As I will explain, CFIUS is not a legal-intercept program per se, but it interacts with US legal-intercept programs when a foreign acquisition is subject to FCC Section 214 or CALEA requirements. CFIUS mitigations may also help to prevent surveillance activities by foreign firms that acquire US companies.

How do these surveillance and antisurveillance programs work? To whom do they apply? Do they extend to the overseas operations of US firms? To what extent do they apply to foreign firms whenever they enter the US market?

An analytic summary of these diverse but interrelated US programs does not currently exist in one place. This overview will be useful to compare with similar programs and requirements of other countries, from the United Kingdom and France, to China and Russia—a comparison that also does not currently exist in any public forum.

US companies that participate in such US surveillance programs complain that they are now suffering discrimination and loss of sales as a balkanization of telecommunications markets appears to be taking place. They are calling for a mutual legal assistance treaty (MLAT)—or other new “rules of the road”—to provide transparency and handle conflicting government demands on international companies.

Based on an analysis of US programs, this paper provides a baseline of US practices that might contribute to formulating a prospective mutual legal assistance treaty or alternative rules for legal intercept programs around the world. It should be noted, however, that this paper does not propose to investigate the entire range of covert espionage activities by the US or other countries, nor to examine offensive and defensive measures.
to engage in cyberwarfare, nor to document programs to track and prevent hacking by individuals and governments around the globe.

**Legal Intercept Programs and Reciprocal Surveillance Prevention Efforts**

US regulations designed to permit government agencies to conduct surveillance via US and foreign IT companies to prevent surveillance by foreign companies can be gathered into four groupings. These four groupings interact with one another, but differ in significant aspects.

**Sections 215 (the “Access to Business Records” Provision) and 216 (the “Access to Online Activity” Provision) of the Patriot Act, the FISA Court, and Section 702 of the FISA Amendments Act.** Sections 215 and 216 of the Patriot Act originate in Section 103(a) of the 1978 Foreign Intelligence Surveillance Act, which established the FISA Court system that grants the government permission to conduct electronic surveillance. The act specifies, “The Chief Justice of the United States shall publicly designate seven district court judges from seven of the United States judicial circuits who shall constitute a court which shall have jurisdiction to hear applications for and grant orders approving electronic surveillance anywhere within the United States under the procedures set forth in this Act.”1

The 1978 Foreign Intelligence Surveillance Act gave the government the ability to issue secret warrants for specified items, like records from car rental companies or storage facilities, on the approval of a secret court if they were relevant to a terrorism investigation and if the suspect was a suspected spy or terrorist. At the time there was extensive debate about whether an individual’s library borrowing records might be investigated.

Section 215 of the Patriot Act of 2001—and the reauthorized version of the Patriot Act passed in 2005—broadens the scope by specifying that “tangible things” can be sought, specifically including “books, records, papers, documents, and other items.”2 Section 215 states that such tangible things “must be ‘relevant’ to an authorized preliminary or full investigation to obtain foreign intelligence information or to protect against international terrorism or clandestine intelligence activities.” Section 215 thus removes the limitation that records could be sought only for a suspected spy or terrorist. The only remaining limitation is that the secret warrant has to be relevant to a national security investigation.

Warrant applications under the Foreign Intelligence Surveillance Act are drafted by attorneys in the General Counsel’s Office at the National Security Agency at the request of an officer of one of the federal intelligence agencies. Both the request for a warrant and the court’s ruling are classified.

Section 215 established congressional oversight for the FISA program, requiring the Department of Justice to conduct an audit of the program and how effectively Section 215 was used and to submit an unclassified report on the audit to the House and Senate Committees on the Judiciary and Intelligence.

Section 215 orders may be combined with requests under other provisions of the Patriot Act, such as Section 216, which governs access to online activity such as email contact information or Internet browsing histories. This includes trap and trace devices inserted on packet-switched data networks. Section 216 allows the agency that applied for the order to compel any relevant person or entity providing wire or electronic communication service to assist with the surveillance.

Sections 215 and 216 apply to “any provider of a wire or electronic communication service, landlord, custodian, or other person that provides any information, facilities, or technical assistance.” There is no stipulation about the nationality of the provider, so these sections must logically apply to foreign companies operating within the United States. One must suppose therefore that these sections apply, for example, to China Telecom (which entered the US market in 2002) and to China Unicom (which entered the US market in 2003) and will apply to China Mobile if the latter manages to get FCC Section 214 approval to operate in the United States. Similarly, one must suppose that they will also apply to Chinese company Alibaba.

Section 225 confers legal immunity upon those who assist with the implementation of Sections 215 and 216. Section 702 of the FISA Amendments Act complements Sections 215 and 216 of the Patriot Act in important respects. In June 2013, a copy of a top-secret...
warrant, issued by the FISA Court on April 25, 2013, was leaked to London’s *Guardian* newspaper by US National Security Agency (NSA) contractor Edward Snowden. The warrant orders Verizon Business Network Services to provide a daily feed to the NSA containing “telephony metadata”—comprehensive call detail records, including location data about all calls in its system, including those that occur “wholly within the United States including local telephone calls.”

This revelation led to the disclosure of a NSA program named PRISM that allows the NSA and the Federal Bureau of Investigation (FBI) to tap directly into the central servers of nine leading US Internet companies, extracting audio, video, photographs, emails, documents, and connection logs that enable analysts to track a person’s movements and contacts over time. Besides Verizon, the companies include Google, Facebook, Skype, and Apple.

When queried about the legal basis for PRISM, the US government cites Section 702 of the FISA Amendments Act, a law first passed in 2008 and reauthorized in 2012. Section 702 allows the government to acquire foreign intelligence by targeting non-US persons “reasonably believed” to be outside US borders. Under Section 702, the FISA Court’s role is more limited than for the Patriot Act. Section 702 does not allow the intentional surveillance of US persons, but the government is not required to go before the court to obtain individual surveillance orders. Instead, the court approves “targeting” and “minimization” to limit the amount of information about law-abiding Americans that is intercepted, retained, and disseminated. Some information about Section 702 programs must be reported to Congress’s intelligence and judiciary committees, including significant legal opinions of the FISA Court. However, these reports are classified and not shared broadly.

A key question regards what standing IT companies and individuals enjoy before the FISA Court. In particular, do IT companies have a say in the process of demanding access to user data? In theory, the answer is yes. If served with an order under Section 215, 216, or 702 demanding records, a communications provider can challenge it. Like all proceedings before the FISA Court, such a challenge would be secret (as is compliance with the court’s orders). The companies, meanwhile, are prohibited from disclosing information about the government’s requests to the public through gag orders. Companies may also challenge these gag orders. But the required secrecy of the court’s proceedings makes it impossible for an outsider to know whether or how often companies might have mounted any challenge to the FISA Court orders or what the outcome might have been.

In January 2014, President Barack Obama ordered the Justice Department to allow tech companies such as Facebook, Microsoft, Google, LinkedIn, and Yahoo to disclose the total number of FISA Court orders they receive annually and the total number of users those requests affect. Previously, these companies had been prohibited from disclosing anything about the government’s requests for information.

What is the status of individuals whose records are being investigated? Persons whose records are targeted do not have the right to appear before the FISA Court. Moreover, since the surveillance programs are classified, targeted persons generally have no way of knowing that their records are the subject of specific government scrutiny. Although individuals or organizations can submit requests under the Freedom of Information Act or the Privacy Act asking for information about whether the government has been spying on them or others, commentators on Sections 215, 216, and 702 report that these requests are likely to be denied.

In a related but distinct case, a US court has ruled that Microsoft must turn over records stored in Ireland of an individual who is a suspect in a criminal case. With support from Apple, AT&T, and Verizon, Microsoft has protested this extraterritorial application of US law. German users have warned that they would stop using Microsoft products if the case is upheld on appeal. (The
legal basis for this ruling is the Stored Communications Act, 18 U.S.C., 2701, not the Patriot Act.)

Critiques of Sections 215, 216, and 702 raise a number of important issues. The American Civil Liberties Union (ACLU), for example, notes that Sections 215 and 216 expand the US government’s power to spy on ordinary people living in the United States, including US citizens and permanent residents, without customary restraints.\(^5\)

The FBI need not show probable cause, nor even reasonable grounds to believe that the person whose records it seeks is engaged in criminal activity, nor have any suspicion that the subject of the investigation is a foreign power or agent of a foreign power. The FBI can investigate United States residents based in part on their exercise of First Amendment rights, and it can investigate non–United States residents based solely on their exercise of First Amendment rights. For example, argues the ACLU, the FBI could spy on a person because it does not like the books she reads or the websites she visits. It could spy on her because she wrote a letter to the editor that criticized government policy.

The ACLU notes that those served with Section 215 or 216 orders are prohibited from disclosing the fact to anyone else. Subjects of surveillance are never notified that their privacy has been compromised. If the government had been keeping track of what books a person had been reading or what websites she had been visiting, notes the ACLU, the person would never know.

The FISA deliberations about granting a Section 215 or 216 order are granted ex parte—that is, the FISA Court hears only the government’s argument—in the absence of, without notification of, and without any chance for rebuttal or counterargument from those who are targets of surveillance. A further problem with the ex parte structure, Elizabeth Goitein, codirector of the Liberty and National Security Program at the Brennan Center for Justice in New York, points out, is that when traditional courts make mistakes, the losing party has the right to appeal and the erroneous decision is reversed. “That process cannot happen when a secret court considers a case with only one party before it,” she argues.\(^6\)

Some critics point out that it is extremely rare for the court to turn down FISA warrant requests.\(^7\) During the 25 years from 1979 to 2004, 18,742 warrants were granted, while just four were rejected. Fewer than 200 requests had to be modified before being accepted, almost all of them in 2003 and 2004. The four rejected requests were all from 2003, and all four were partially granted after being submitted for reconsideration by the government. Few, if any, requests had to be modified before 2000. During the next eight years, from 2004 to 2012, more than 15,100 additional warrants were granted, with an additional seven rejected. In all, over the entire 33-year period, the FISA Court has granted 33,942 warrants, with only 11 denials—a rejection rate of 0.03 percent of the total requests.

But the accusation that the FISA Court is a rubber-stamp court has been rejected by Robert S. Litt, general counsel of the Office of the Director of National Intelligence:

When [the Government] prepares an application for [a section 215 order, it] first submit[s] to the FISA Court what’s called a “read copy,” which the court staff will review and comment on. [A]nd they will almost invariably come back with questions, concerns, problems that they see. And there is an iterative process back and forth between the Government and the [FISC] to take care of those concerns so that at the end of the day, we’re confident that we’re presenting something that the [FISC] will approve. That is hardly a rubber stamp. It’s rather extensive and serious judicial oversight of this process.\(^8\)

A further issue of concern is the ability of the FISA Court to create its own interpretations of the US statutes under which it operates and to establish its own precedents. After resigning his position on the FISA Court, Judge James Robertson criticized the court for being allowed to craft a secret body of law.\(^9\)

To summarize, Section 215 allows electronic surveillance by securing access to the data banks of companies. Section 216 allows the insertion of electronic surveillance mechanisms (tap and trace devices) into the IT systems of IT companies. Sections 215 and 216 do not, however, appear to require IT companies to deliberately design hardware and software systems so as to allow backdoors and trapdoors through which US intelligence agencies can conduct surveillance, unlike CALEA.
The FCC, Section 214 Licenses, and “Team Telecom.” Any telecommunications provider (including facilities-based carriers, resellers, prepaid calling card providers, and wireless service providers) that offers calling services between the US and foreign points must obtain a certificate of authority under Section 214 of the Communications Act. It is unlawful to offer or advertise services allowing international calling without first obtaining a Section 214 license to offer international telecommunications service.

Each Section 214 application that includes 25 percent direct or indirect foreign ownership is reviewed by the FCC’s International Bureau and, as part of the bureau’s processing, requires approval from Team Telecom, a working group of representatives from federal agencies outside the Federal Communications Commission. This group scrutinizes the application “for potential national security, law enforcement, and public interest concerns.” Team Telecom is a working group of federal agencies outside the Federal Communications Commission. Staff from the Department of Homeland Security, the Department of Justice (including the FBI), and the Department of Defense colead Team Telecom. (In contrast to CFIUS, Team Telecom is composed entirely of security-related agencies and does not include representation by the US Department of the Treasury, US Department of State, or Office of the US Trade Representative.)

Team Telecom assesses each communications service provider applicant through a list of triage questions that ask for details on the applicant’s ownership structure, senior leadership, network topology, service offerings, customer base, and technical capabilities for lawful electronic surveillance. Depending on the risk level assigned to the applicant, Team Telecom may impose certain risk mitigation measures. The FCC reports that one of the most common risk mitigation measures is to have the applicant install a repository of its customer data records on US soil. That would give US courts jurisdiction over the data for purposes of ordering any disclosures for a national security or law enforcement investigation. Similarly, Team Telecom may ask the applicant to make a resident US citizen available for service of due process from a law enforcement agency that needs to investigate the customer data.

Operating as a Section 214 licensee triggers a range of ongoing federal compliance obligations. One requirement is to promptly report to the FCC any substantial changes in ownership, transfers of control, or other changes in the regulatory status of the license. Thus, Section 214 licensing is not a one-step, one-time obligation but, rather, a mechanism for continuous review.

A Section 214 licensee’s commitments to Team Telecom are documented in one of two ways: a letter of assurances or a national security agreement. A letter of assurances is used in cases where only basic risk mitigation measures are needed, whereas a national security agreement codifies more elaborate measures in higher-risk assessment cases. A national security agreement, which is a formal, detailed contract, may subject an applicant to periodic law enforcement agency audits and regular reporting requirements. In some cases a national security agreement has required the licensee to have members of its security staff undergo FBI background investigations for purposes of obtaining security clearances.

Some Section 214 applicants are subject to CALEA, the US statute that requires telecommunications carriers to deliberately design their equipment and networks to enable penetration and surveillance by US agencies. In those cases, Team Telecom would expect the applicant to comply with CALEA.

But Team Telecom can impose requirements beyond CALEA obligations. An early case that illustrates Team Telecom’s capabilities is the security agreement for Global Crossing, a company whose fiber-optic network connected some 27 nations on four continents. Global Crossing went bankrupt in 2002 after struggling to handle the burden of $12 billion in debt, and two companies, one from Singapore and a second from Hong Kong, struck a deal to buy a majority stake. Team Telecom forced the Hong Kong partner to withdraw out of concern that the Chinese government would “gain access to US surveillance requests and infrastructure.” The remaining investor, Singapore Technologies Telemedia, eventually agreed to a slate of Team Telecom demands, including allowing half of the board of directors of a new subsidiary managing the undersea cable network to consist of American citizens with security clearances. Those US directors would oversee
a head of network operations, a head of global security, a general counsel, and a human resources officer—all of whom also would be US citizens with security clearances. Team Telecom retained the right to veto any appointments to those jobs or any appointments to US citizen directorships.

In 2011, Singapore Technologies Telemedia sold Global Crossing to Level 3 Communications, a US company based in Colorado. But the Singaporean company maintained a minority ownership stake, helping trigger an additional round of reviews by Team Telecom and a revised network security agreement that added several new conditions.

The FCC will not grant any Section 214 petition that is not approved by Team Telecom. This gives the latter great leverage in “negotiating” with IT companies. Talks with Team Telecom typically involve little give and take; notes one practitioner, “It’s like negotiating with the Motor Vehicle Department.”

The procedures, investigations, and findings of Team Telecom are not usually made public, although network security agreements are published on the FCC website. Upon finishing its review, Team Telecom then communicates its determination to the FCC’s International Bureau. Team Telecom does not act pursuant to any specific legal basis. The FCC explains that in the Foreign Participation Order of 1997 it set forth its policy for reviewing applications, but states that the FCC defers to “the expertise of the Executive Branch,” embodied in Team Telecom representatives, “for potential national security, law enforcement, and public interest concerns.”

The Communications Assistance for Law Enforcement Act (CALEA). The US Federal Communications Commission described the Communications Assistance for Law Enforcement Act as follows:

In response to concerns that emerging technologies such as digital and wireless communications were making it increasingly difficult for law enforcement agencies to execute authorized surveillance, Congress enacted CALEA on October 25, 1994. CALEA requires all telecommunications carriers to ensure that equipment, facilities, or services that allow a customer or subscriber to “originate, terminate, or direct communications,” enable law enforcement officials to conduct electronic surveillance pursuant to court order or other lawful authorization. CALEA is intended to preserve the ability of law enforcement agencies to conduct electronic surveillance by requiring that telecommunications carriers and manufacturers of telecommunications equipment modify and design their equipment, facilities, and services to ensure that they have the necessary surveillance capabilities as communications network technologies evolve.13

The Electronic Frontier Association rephrases the last sentence of this description in more contemporary parlance to say that CALEA forces all broadband Internet and interconnected Voice over Internet Protocol (VoIP) services to become wiretap-friendly, requiring companies to design and manufacture surveillance-accessible technologies that build backdoors into all Internet communications.14 Surveillance must be made available on a real-time or near-real-time basis and provide continuity of interception as new equipment and software are installed over time.

Section 103 of the CALEA legislation expands on the surveillance requirements:

A telecommunications carrier shall ensure that its equipment, facilities, or services . . . are capable of (1) expeditiously isolating and enabling the government . . . to intercept . . . all wire and electronic communications carried by the carrier within a service area to or from equipment, facilities, or services of a subscriber of such carrier concurrently with their transmission to or from the subscriber’s equipment, facility, or service, or at such later time as may be acceptable to the government; (2) expeditiously isolating and enabling the government . . . to access call-identifying information . . . (A) before, during, or immediately after the transmission of a wire or electronic communication (or at such later time as may be acceptable to the government); . . . (3) delivering intercepted communications and call-identifying information to the government . . . in a format such that they may be transmitted by means of equipment, facilities, or services procured by the government to a location other than the premises of the carrier; and (4) facilitating authorized communications interceptions and access to call-identifying
information unobtrusively and with a minimum of interference with any subscriber’s telecommunications service and in a manner that protects . . . information regarding the government’s interception of communications and access to call-identifying information. . . .

A telecommunications carrier that is a provider of commercial mobile service . . . offering a feature or service that allows subscribers to redirect, hand off, or assign their wire or electronic communications to another service area or another service provider or to utilize facilities in another service area or of another service provider shall ensure that, when the carrier that had been providing assistance for the interception of wire or electronic communications or access to call-identifying information no longer has access to the content of such communications or call-identifying information . . . within the service area in which interception has been occurring as a result of the subscriber’s use of such a feature or service, information is made available to the government (before, during, or immediately after the transfer of such communications) identifying the provider of a wire or electronic communication service that has acquired access to the communications.15

Finally, CALEA states that a telecommunications carrier shall not be responsible for decrypting, or ensuring the government’s ability to decrypt, any communication encrypted by a subscriber or customer unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication. This is a backhanded way of saying that IT companies that provide encryption services must ensure that the US government can decrypt all messages that use the encryption services they provide to customers.

One of the companies most often named in connection with CALEA’s requirements to place backdoors and other surveillance mechanisms within hardware and software is Cisco, the leading US provider of routers and switches. In August 2013, the Wall Street Journal revealed that CALEA’s reach extended even to foreign telecommunication companies that had merged with or acquired the assets of US-based companies.16 Before being given the green light for their mergers with or purchases of US firms, Alcatel-Lucent, Nokia, and Ericsson, each had to commit to the federal government to adhere to the terms of CALEA, according to the Wall Street Journal, and give unfettered access to their equipment.

\[\text{In all, over the entire 33-year period, the FISA Court has granted 33,942 warrants, with only 11 denials—a rejection rate of 0.03 percent of the total requests.}\]

But this “exposé” should not be surprising. When queried about who must comply with CALEA, the Department of Justice states, “all telecommunications carriers or other entities engaged in the transmission or switching of wire or electronic communications as a common carrier for hire.”17 Thus, CALEA requirements apply to all foreign telecom service providers or switching equipment suppliers operating in the United States, whether or not they acquire US entities in the process of entering the American market. The foreign parent firm must know about the requirement to design hardware and software to permit surveillance; specific requests for intercepts must be made to an appropriately cleared US citizen in the firm and kept closely held.

To verify compliance, all telecommunications carriers must file and maintain up-to-date System Security and Integrity plans—which demonstrate surveillance-friendly hardware and software—with the FCC, including when their switching equipment, facilities, or service are replaced, significantly upgraded, or otherwise significantly modified.

A telecommunications carrier may comply with CALEA in three different ways. First, the carrier may develop its own compliance solution for its unique network. Second, the carrier may purchase a compliance solution from vendors, including the manufacturers of the equipment it is using to provide service. Third, the carrier may purchase a compliance solution from an expert third party.

There is a close interconnection between CALEA requirements and FCC Section 214 requirements. Team Telecom ensures all IT companies that provide services between the US and foreign locations and thus
need a Section 214 license from the FCC to do business are in compliance with CALEA.

The Committee on Foreign Investment in the United States (CFIUS). CFIUS is an interagency group led by the Treasury Department whose responsibility is to ensure acquisitions of US firms by foreigners do not pose a threat to US national security. CFIUS does not have a mandate to require foreign acquirors to participate in US legal-intercept programs per se, but the committee’s mitigation requirements interact with US legal-intercept mandates when a foreign acquisition is subject to FCC Section 214 or CALEA requirements. One of the national security issues that CFIUS addresses is how to prevent surveillance activities by foreign firms that acquire US companies.

The secretary of the Treasury is the chairperson of CFIUS, and notifications of proposed foreign acquisitions are received, processed, and coordinated at the staff level by the staff chairperson of CFIUS, who is the director of the Office of Investment Security in the Department of the Treasury. The members of CFIUS include representatives from the Department of the Treasury (chair), Department of Justice, Department of Homeland Security, Department of Commerce, Department of Defense, Department of State, Department of Energy, Office of the US Trade Representative, and Office of Science and Technology Policy, as well as other agencies from time to time, such as the National Security Council. The director of national intelligence is a nonvoting ex officio member of CFIUS, coordinating all assessments and input from US intelligence agencies.

Filing for a CFIUS review by foreign companies before an acquisition is technically voluntary. During the review period, CFIUS members examine the transaction to identify and address any national security concerns that arise as a result of the transaction. During the review period, CFIUS members, through the committee chair, may request additional information from the involved parties.

Once a case of proposed acquisition is filed, CFIUS confidentially investigates the transaction and reports to the president of the United States on its findings. The president has the ultimate authority to block or allow any transaction. Historically, the president has blocked only two proposed acquisitions following a CFIUS review. However this statistic may be somewhat misleading since more transactions are discouraged or become untenable prior to a formal committee finding. If a foreign firm does not file a notice to CFIUS regarding a proposed transaction, then CFIUS can initiate its own investigation and subsequently order a divestment.

The CFIUS process involves a 30-day investigation, and the majority of transactions are cleared in this time period. But the committee may initiate an additional 45-day investigation if the lead agency requests such, if one agency finds a national security concern, if the transaction involves foreign government control, if the transaction concerns critical infrastructure, or if CFIUS needs more time. This second 45-day investigation is mandatory if the foreign acquiring firm has ties to a foreign government or involves critical infrastructure in the United States. The president has 15 days to evaluate CFIUS findings and allow or prohibit the transaction.

CFIUS reviews proposed acquisitions of US firms “to determine the effects of the transaction[s] on the national security of the United States,” but does not define “national security.” The Foreign Investment and National Security Act statute offers an extensive menu of precepts and parameters to consider. To help clarify its procedures, the US Department of the Treasury, as CFIUS chair, published “Guidance Concerning the National Security Review Conducted by CFIUS” in the Federal Register on December 8, 2008. This guidance explains that CFIUS identifies all national security considerations (facts and circumstances that have potential national security implications) to assess whether the transaction poses a national security risk (whether the foreign person that exercises control over the US business as a result of the transaction might take action that threatens to impair US national security). In analyzing whether the transaction poses a national security risk, CFIUS assesses whether a foreign person has the capability or intention to exploit or cause harm (whether there is a threat) and whether the nature of the US business or its relationship to a weakness or shortcoming in a system, entity, or structure creates susceptibility to impairment of US national security (whether there is a vulnerability). National security risk is a function of the interaction between threat and vulnerability and the potential consequences of that interaction for
US national security. This national security risk assessment is conducted based on information provided by the parties, public sources, and government sources, including a classified national security threat assessment that the director of national intelligence prepares for CFIUS within 20 days after a notice of a transaction is accepted.

If CFIUS finds that a proposed acquisition presents national security risks and that other provisions of law do not provide adequate authority to address the risks, then it may enter into an agreement with, or impose conditions on, parties to mitigate such risks. Mitigating measures that can be imposed on the acquiring firm include allowing US citizens to run only certain departments or insisting the firm give up control of or divest certain operations. In 2013, for example, the Chinese international energy company China National Offshore Oil Corporation (CNOOC) proposed to buy Nexen, a Canadian energy company that had significant operations in the Gulf of Mexico. The transaction had to be approved by both Canadian and US authorities. CFIUS demanded that CNOOC relinquish operating control of its gulf activities (presumably because of a threat of monitoring maritime operations in the gulf although, as I will explain, the alleged nature of the national security threats is not disclosed to the parties), but the CNOOC parent was allowed to collect the revenue from gulf operations.

CFIUS does not make its national security determinations public nor does it provide them on a confidential basis to the parties. CFIUS contends that publishing its national security determinations might reveal sources and methods of US intelligence gathering. As a result, foreign companies do not know what might be held against them and are not able to rebut or defend themselves. There may be, however, a sequence in which CFIUS poses questions or asks for more information and the parties respond.

Foreign companies have not enjoyed due process as part of the CFIUS investigation. On July 15, 2014, the US Court of Appeals for the DC Circuit held that review by CFIUS of a wind farm investment by Chinese-owned Ralls Corporation near a US military base and the subsequent unwinding of the investment deprived the Chinese investor of due process. If upheld, the ruling may require changes in how CFIUS handles its determinations. The due process ruling applied only to the unclassified portion of the CFIUS determination.

When the foreign acquisition of a US firm includes a Section 214 application to provide telecom services, this triggers parallel national security reviews by CFIUS and Team Telecom. As I have noted, CFIUS investigates the national security implications of foreign acquisitions of US firms in all sectors, of course, not just IT, telecommunications, and electronics.

---

**IT companies that provide encryption services must ensure that the US government can decrypt all messages that use the encryption services they provide to customers.**

Simultaneous national security investigations by Team Telecom and CFIUS are found, for example, in the 2013 merger of SoftBank with Sprint Nextel, which in turn was seeking to acquire mobile and fixed broadband provider Clearwire. Together, Team Telecom and CFIUS extracted extensive concessions from the parties. First, the Departments of Defense, Homeland Security, and Justice secured the right to review and veto new equipment purchases in certain circumstances. The companies were required to appoint a new Sprint Nextel board member, to be approved by the US government, to supervise national security compliance. Finally, the US government reserved the right over a period of time to order SoftBank to remove any equipment in the networks of Sprint Nextel and Clearwire that were supplied by Chinese equipment vendor Huawei Technologies. All told, this set the precedent for Team Telecom and CFIUS to control a communication company’s management composition and its choice of equipment suppliers.

The SoftBank–Sprint Nextel case illustrates that CFIUS threat assessments, like the threat assessments of other parts of the US government (including the US Congress), often reflect the conviction that singling out particular companies by nationality of their headquarters and excluding (or regulating) their participation in US IT markets resolves the vulnerability...
of US IT networks. But in a world of globalized supply chains, the exclusion or regulation of foreign companies on the basis of their national origins is not an effective approach to ensure the integrity of US IT systems. Today, all IT corporations outsource the production of hardware and software to China, India, Israel, and Russia, as well as Taiwan, Malaysia, Thailand, and Mexico. The potential for inserting trapdoors, backdoors, and surveillance mechanisms in hardware or software is ubiquitous. What is needed is a multilateral nondiscriminatory system to ensure the integrity of equipment and software—and patches and upgrades—from all sources.

What is needed is a multilateral nondiscriminatory system to ensure the integrity of equipment and software—and patches and upgrades—from all sources.

More broadly, leading US companies have appealed to the US government to ensure transparency, avoid discrimination, and deal with conflicts among national governments by negotiating a Mutual Legal Assistance Treaty (MLAT) to cover legal intercept and other national security screening mechanisms.

Toward a Multilateral Framework for Legal Intercept and Other National Security Screening Mechanisms

US IT companies and suppliers of IT goods and services report discrimination toward and loss of sales by governments and private buyers in other countries that want to avoid US government surveillance. They warn of the balkanization of telecommunication markets around the world.

Eight of the largest US multinational corporations (Apple, Google, Microsoft, Facebook, Yahoo, LinkedIn, Twitter, and AOL) cosigned a letter to President Barack Obama and members of Congress outlining five principles to govern surveillance practices. Two of those principles are transparency about government demands and mechanisms to avoid conflict among governments. To pursue these two principles, the companies argue, “There should be a robust, principled, and transparent framework to govern lawful requests for data across jurisdictions, such as improved mutual legal assistance treaty—or ‘MLAT’—processes. Where the laws of one jurisdiction conflict with the laws of another, it is incumbent upon governments to work together to resolve the conflict.”

An MLAT is an agreement between two or more countries for the purpose of enforcing public laws and preventing criminal or other illegal behavior. They are currently used in countering tax avoidance, money laundering, and terrorist funding activities. Ultimately the larger goal might be not just to avoid conflict of laws, but also to provide a multilateral framework for lawful surveillance and national security screening among states.

In the same vein, Cisco CEO John Chambers complained to President Obama about reports that the NSA intercepts US-made networking hardware on the way to foreign customers to install modifications to allow US government surveillance. The reports included a photograph of packages of Cisco equipment being opened at an NSA facility, reconfigured with backdoor software, and repackaged for delivery overseas. “We simply cannot operate this way,” Chambers wrote to the president. “If these allegations are true, these actions will undermine confidence in our industry and in the ability of technology companies to deliver products globally.” Chambers called for “a new set of ‘rules of the road,’ to ensure that appropriate safeguards and limits exist that serve national security objectives, while at the same time meet the needs of global commerce.”

To move in the direction of a MLAT for lawful surveillance—or other “rules of the road”—it would be necessary to know precisely what regulations and directives govern lawful surveillance in other countries around the world. Such information is not now publicly available. And those who may know a good deal about such regulations and directives in other countries—such as Anne Neuberger, director of the NSA’s Commercial Solutions Center and the agency’s principal liaison with technology companies—warn, “Before anyone makes a decision to stop using the services of U.S. communications companies, we’d strongly...
encourage them to take a look at the lawful intercept regimes of various countries around the world. I know you will find that U.S. law provides some of the strongest protections for the privacy of users.\textsuperscript{24}

Beginning, therefore, with what is known about US regulations and practices regarding legal intercept, a multilateral framework would have to cover several areas (table 1).

Rather than waiting for long and arduous negotiation of a MLAT, however, companies may launch a counteroffensive on their own. Indeed, some companies are clearly already taking matters into their own hands. On September 17, 2014, Apple announced a new privacy policy, in which its latest mobile operating system, iOS8, is designed so as to prevent Apple—or anyone but the device’s owner—from accessing content on the device, even if the company is served by a legitimate warrant. The new generation of iPhones and iPads will not allow Apple to bypass the owner’s passcode and extract data in response to a government request, unlike in the past. Apple will still be able to access any user data stored on iCloud, so law enforcement could, with a warrant, compel the company to turn over iCloud files. But if the files exist only on a user’s device, not on the cloud, Apple will be incapable of permitting access to those files. Google quickly followed suit for its Android operating system.

The major competitors of Apple and Google from Europe, Korea, and China are almost certain to do the same, defying not only US intercept regulations but also regulations of other governments around the world. A new generation of mobile devices from Samsung, Ericsson, Motorola, and competitors will frustrate the surveillance demands of France, China, Russia, and other countries around the globe.

The analysis presented here aims to provide a baseline from which a multilateral effort might be launched to coordinate lawful surveillance regulations around

| Regulations Backed by Legislation? | Yes |
| Regulations Public (Not Secret)? | Yes |
| Regulations Apply to Foreign As Well As Domestic Firms? | Yes |
| Court Warrants Required? | Yes |
| Court Warrants Public (Not Secret)? | No |
| Court Warrants Issued Ex Parte? | Yes |
| Targets of Investigation Notified? | No |
| Targets of Investigation Entitled to Due Process? | ?? |
| Requirement for Access to Domestic Databases? | Yes |
| Extraterritoriality: Requirement for Access to Offshore Databases? | Yes |
| Requirement to Design Hardware and Software to Allow Surveillance? | Yes |
| Requirement to Turn Over Encryption Keys | Yes |
| Right to Block Entry of Foreign Firms into Domestic Market? | Yes |
| Right to Block Foreign Acquisitions of Domestic Firms? | Yes |
| Right to Require Foreign Firms to Divest Certain Assets/Operations? | Yes |
| Right to Require Foreign Firm to Appoint Certain Board Members? | Yes |
| Right to Require Foreign Firms to Exclude Certain Suppliers of Equipment and Services? | Yes |

Source: Author’s research compiled in this paper.
the world. The alternatives—segmentation of IT markets along nation-state lines or arbitrary efforts by international IT companies to render themselves unable to obey government directives—will end up being not only vastly costly but also ineffective in balancing respect for privacy with legitimate concerns about crime and terrorism.
Notes


11. Ibid.


About the Author

Theodore H. Moran holds the Marcus Wallenberg Chair in International Business and Finance at the School of Foreign Service, Georgetown University, where he teaches and conducts research at the intersection of international economics, business, foreign affairs, and public policy. He is a consultant to the United Nations, diverse governments in Asia and Latin America, and the international business and financial communities. From 2007 to 2013, he served as associate to the National Intelligence Council Panel on international business issues. Moran is also a member of the International Advisory Council of Huawei and a nonresident senior fellow at the Peterson Institute for International Economics and at the Center for Global Development.

Moran’s recent books include *Foreign Direct Investment in the United States: Benefits, Suspicions, and Risks with Special Attention to FDI from China* (with Lindsay Oldenski, Peterson Institute for International Economics, 2013) and *Foreign Direct Investment and Development: Launching a Second Generation of Policy Research: Avoiding the Mistakes of the First, Reevaluating Policies for Developed and Developing Countries* (Peterson Institute for International Economics, 2011).

Acknowledgments

I wish to thank Claude Barfield, Nova Daly, Stephen Heifetz, and Clay Lowrey for helpful comments and corrections. Any errors that remain are my own.