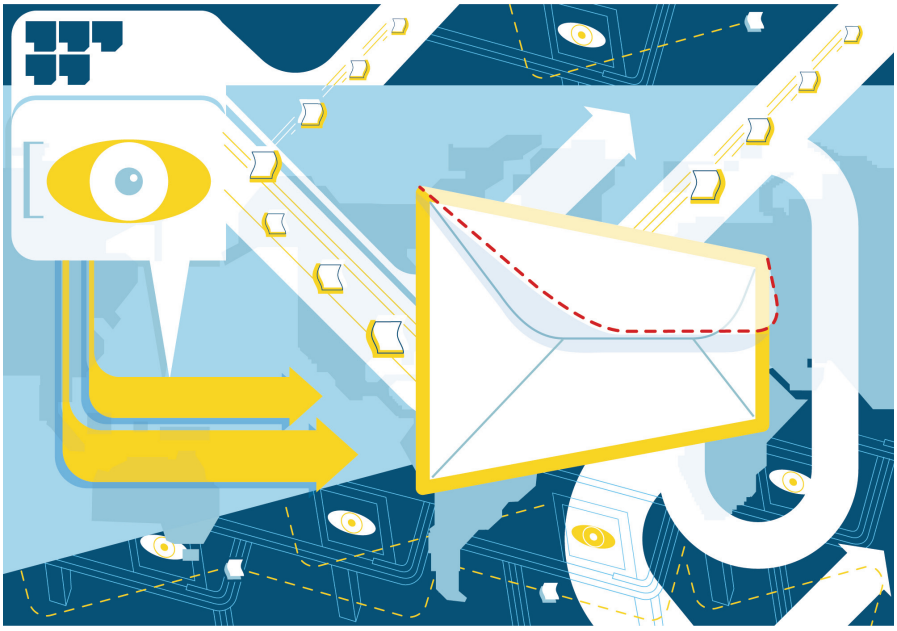
DOI:10.1145/1461928.1461940

Kristina Irion

Privacy and Security
International Communications Surveillance

Aren't we all foreigners when our Internet traffic transits through other countries and is subject to regional intelligence-gathering policies?

When you send email, do you know through which countries your communication will be routed? In a world where countries use the Internet to gather intelligence from communications traffic that transits local facilities, this question has become increasingly important for Internet users—individuals and businesses alike. Such interception is an established investigative tool of intelligence services and law enforcement agencies all over the world provided for by domestic laws. For governments concerned with national-security threats, the exploitation of all available sources for intelligence gathering seems obvious. This surveillance is constantly being expanded—to the detriment of communications privacy. Countries are increasingly adopting legislation that provides for preventive surveillance and the massive collection of communications data without either adequate procedural limitations or strict oversight of the activities. In the worst case governments stretch—or even ignore—existing rules in order to facilitate intelligence gathering no matter what.



The fact that Internet traffic is supranational in character offers a promising new avenue for intelligence gathering by targeting international communications originating from, terminating in, or simply passing through a given country and subjecting it to the local standards of legal interception. Unlike the public switched telephony network (PSTN), which delivered only the destined traffic to the international gateways, Internet traffic is not confined to the territory of a state and is more likely to cross borders while in transit. Not long ago the overwhelming majority of data flowed through the U.S., where the world's top Internet backbone providers' switching equipment was located (the situation has since changed somewhat). The U.S. was therefore in the position of being able to exercise control over most of the world's information transmitted via the Internet.

In 2005 the U.S. National Security Agency's warrantless wiretapping, a program authorized by the Bush administration, was disclosed. Afterward the government pursued legislation to expand surveillance powers. The short-lived 2007 Protect America Act and its immediate successor, the Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008, permit warrantless interception of international communications during transit through the U.S. and the targeting of non-U.S. persons reasonably believed to be located outside the U.S. Under the latter U.S. act, the highest level of protection is afforded to purely domestic communications, interception of which would require a warrant whereas international communications (with at least one foreign end-

ILLUSTRATION BY CELIA JOHNSON

point) are more exposed to surveillance activities. If this logic were to be adopted worldwide, a citizen would have privacy of communications only in the nation in which they had citizenship—and then only if the communications remained fully within the nation's borders, a situation not always guaranteed when using the decentralized architecture of the Internet. From the perspective of all other countries the same Internet communications would be treated as foreign communications and are thus susceptible to surveillance when on transit through their territories. This privacy threat is not just abstract, but is a realistic assessment in a communications environment powered by Internet technologies.

International adoption of the Internet has diminished the strategic predominance of the U.S. over the Internet's core infrastructure, while the percentage of international transit traffic carried via U.S. routes continues to decrease.[3] Many regions of the world are catching up, setting up new intra-regional hubs for Internet exchanges that carry international Internet traffic.[3] Europe has been mostly self-sustaining for some time now and is also attracting the majority of traffic from neighboring regions like Africa and the Middle East.

At the same time, the European protection of the confidentiality of communications as a revered fundamental value in the national constitutions has seen some severe setbacks. It remains to be seen whether electronic communications are any better protected against sweeping legal interception. The European Union (EU) Directive mandating data retention laws in the EU Member States largely compromised the expectation of privacy when communicating electronically. Providers of telephony, email services, and Internet access are required to log communications metadata—the information on who is calling whom when and for how long—and retain these records for up to two years. Such preemptive storing of such data for every user based within the territory of the EU is "just in case." As a consequence, the substance of this fundamental right is condensed to communications content, while the circumstances of individual communications via electronic means are subject to data retention. The EU Data Retention rule, however, only applies to metadata of Internet email and telephony that originates and/or terminates within the EU. Communications content and mere transit of international traffic through European Internet exchanges are not affected by this rule.

Neighboring countries are no less outraged about Sweden's approach to international surveillance, which affects their national communications sectors.

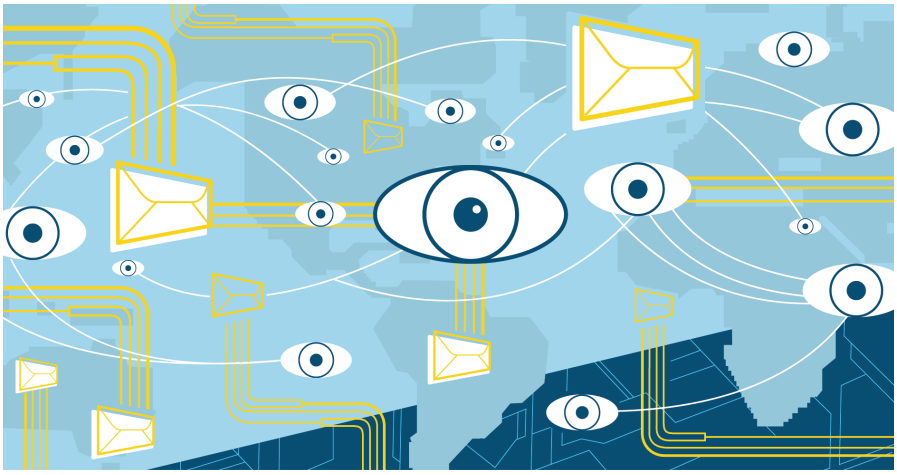
However, a number of European countries do maintain their own domestic surveillance programs that also target international communications, with Sweden recently catching up—and now overtaking—other nations. In June 2008, the Swedish parliament passed the New Signal Surveillance Act or FRA law, as it had been dubbed, which grants, in the name of national security, Sweden's National Defense Radio Establishment (Försvarets Radioanstalt—FRA) the power to access the complete Internet and telephone communications in and out of Sweden. The bill, which took effect at the beginning of this year, obliges all operators of Internet exchange points in Swedish territory to channel traffic though FRA's facilities. Sweden's move toward international communications surveillance went far beyond existing legal standards in other European countries. In his personal blog, Peter Fleischer, Google's Global Privacy Counsel, compared the Swedish government initiative to those of governments from China to Saudi Arabia and the U.S. eavesdropping program.[1]

The passage of the Swedish law involved some odd circumstances. The Swedish center-right alliance in power succeeded with a very narrow majority of 143 votes to 138 in favor of the law after the introduction of some last-minute changes to address oversight of FRA's surveillance activities. Even after this, the first version of the FRA law might have clashed with the privacy protection granted under the European Convention of Human Rights (ECHR). The law's language is vague and its provisions might exceed what is necessary in a democratic society. In order to address some of these obvious weaknesses, the parliament asked the government to propose further amendments in a number of areas by autumn 2008, well before the original law would have taken effect.[5] It seems quite unusual though that a law was passed along with a mandate to fix the flaws even before the law takes effect.

From a political perspective, the surveillance initiative has been a disaster for the Swedish government: its sweeping effect upset political allies, voters, businesses, and neighboring countries alike. Beginning with the legislative process, opposition to the law only grew once the law was adopted. By now awareness about the issue is extremely high and the government has lost significant credibility with the public. The Swedish daily newspaper *Expressen* offered a protest email form on its Web site. The newspaper reported six million protest email messages had been generated, a significant number in a nation with a population of nine million (of course, the responses may not all have been from different individuals or from Sweden).

Sweden's reputation as a leading location for international ICT services was considerably damaged. In a public statement, the CEOs of eight major Nordic telecom companies have warned the country that their companies will relocate their activities away from Sweden in order to protect the interests of their international customers and to abide by the legal requirements elsewhere.[4] The Swedish-Finnish telecom operator TeliaSonera has already moved email and Web servers from Sweden. Google and other companies are publicly contemplating withdrawing from Swedish territory as well, a negative trend that would be self-perpetuating.

Neighboring countries are no less outraged about Sweden's approach to international surveillance, which affects their national communications



sectors. Since Sweden serves as a local hub for transit traffic from and to Norway, Finland, and Russia, the wider cross-border impact is evident. For example, Russia would be exposed to the surveillance scheme so long as a significant share of its domestic Internet traffic is routed via Sweden. Apart from the diplomatic distortions these countries have a palpable incentive to bypass Sweden in the near future and connect to other available Internet exchange services or set up their own facilities.

The Swedish example illustrates how not to expand surveillance. It also shows that new surveillance legislation can have repercussions far beyond strict privacy concerns. The subsequent efforts Sweden put into amending the first FRA law were only trying to adjust the sweeping effects it created. The new draft law presented by the government at the end of September last year is significantly more tailored and contains additional safeguards; it introduces a special court designated to authorize signal surveillance requests from the government and the armed forces to FRA.[2]

Because of the possibility that many Big Brothers may be watching, as individuals we lose out when we communicate via the Internet.

European constitutional tradition protects everyone's communications in a country's territory, and thus the same principles and safeguards apply to the legal interception of domestic and international communications. It does not matter where the originator or the recipient of a particular communication are located in order to benefit from the protection guaranteed inside a country. Maintaining the same thresholds for all communications entering a jurisdiction would also help to overcome the expansion of surveillance to foreign individuals and businesses that typically do not have much influence in a legislative process otherwise. For example, it is likely the Swedish people are most concerned about their own rights to privacy in communications and might not be as interested in the rights of foreigners, whose transit communications would be intercepted. Still, their engagement promotes as well the case of foreigners that otherwise do not carry significant political weight.

International agreements that guarantee the right to communications privacy should play a more significant role to uphold the level of protection against unfettered surveillance powers. One example is Article 8 of the European Convention of Human Rights, which provides the right to respect for one's private life and correspondence. More importantly, the possibility to turn to the ECHR for an appraisal of domestic surveillance laws helped to clarify the requirements that legal interception rules have to meet in order to comply with the fundamental right. Its judgments concerning the strategic monitoring schemes, as opposed to monitoring of individual communications, in Germany and the U.K. show that the key to permissible legal interception lies in the precise description of the authority and procedures that would empower a proportionate level of surveillance.[a]

In my opinion, there is no other international mechanism that would compare to the supranational oversight of domestic surveillance laws of the ECHR. Unsurprisingly, many country's national interests point toward intelligence gathering, where internationally enforceable standards for legal interception would just be burdensome. The prospect to access international traffic that is passing through their territories' Internet infrastructure is perceived as an addition to conventional methods of interception.

Because of the possibility that many Big Brothers may be watching, as individuals we lose out when we communicate via the Internet. But the privacy of the individual is only one part of this complex issue; business is another. When international ICT companies choose a regional location for doing business, countries that maintain a proportionate and safeguarded policy regarding legal interception could find themselves with a competitive advantage over neighbors that do not have such policies. And that would ultimately be good for privacy, business, and the security of the nation choosing to adequately protect communications privacy. C

a European Court of Human Rights (ECHR), case of *Weber and Saravia v. Germany*, no. 54934/00, decision of June 29, 2006; case of *Liberty and Others v. the United Kingdom*, no. 58243/00, decision of July 1, 2008.

References

1. Fleischer, P. Sweden and government surveillance (May 31, 2007); http://peterfleischer.blogspot.com/2007/05/sweden-and-government-surveillance.html.
2. Government unites around new FRA law. *The Local* (Sept. 26, 2008); http://www.thelocal.se/14576/20080926/.
3. Markoff, J. Internet traffic begins to bypass the U.S. *The New York Times* (Aug. 30, 2008).
4. Surveillance sweep—A new surveillance law causes a rumpus in Sweden. *The Economist* (July 22, 2008); http://www.economist.com/agenda/displaystory.cfm?story_id=11778941.
5. Sveriges Riksdag. New Signal Surveillance Act (FöU15) (June 18, 2008); http://www.riksdagen.se/templates/R_PageExtended____16402.aspx.

Kristina Irion (irionk@ceu.hu) is an assistant professor in the Department of Public Policy at Central European University in Budapest, Hungary.

ILLUSTRATION BY CELIA JOHNSON