Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

A Survey of Recent Threats to Privacy Rights

It comes as no surprise to some of us that the terrorist events of September 11th 2001 have prompted governments around the globe to strengthen legislative and other attacks on the civil liberties of their citizens. Privacy is one such liberty under jeopardy. For our purposes, we will choose for a working definition of privacy the right to determine when, how and to what extent information about ourselves is communicated to others. This definition reflects the view of privacy that a German court has called "information...

Copyright SANS Institute
Author Retains Full Rights

AD

Beating the IPS?

STONESOFT
Can't be Beat

Learn More

A Survey of Recent Threats to Privacy Rights

It comes as no surprise to some of us that the terrorist events of September 11th 2001 have prompted governments around the globe to strengthen legislative and other attacks on the civil liberties of their citizens. Privacy is one such liberty under jeopardy.

What is privacy?

Philosophical and legal debates over the definition of privacy are still current. A sample of key concepts often cited include:

- the right to be left alone;
- the right to be free of intrusion into private affairs;
- the right to choose the extent to which we're known and subject to others' attentions;
- the right to have our names or likenesses not appropriated;
- the right to avoid public disclosure of private facts.

For our purposes, we will choose for a working definition of privacy ***the right to determine when, how and to what extent information about ourselves is communicated to others***. This definition reflects the view of privacy that a German court has called "informational self-determination". In this paper we will restrict ourselves to comments on governmental attempts to abridge or deny this specific right through two related techniques: the interception of internet communications and the legal restrictions placed on encryption

Is there a right to privacy?

The principle of the right to privacy was established in International law by the United Nations in 1948. Article 12 of the *Universal Declaration of Human Rights* states: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[1] In 1988, this right was re-iterated and expanded on at the 32nd Session of the Commission on Human Rights; Article 17, entitled *The right to respect of privacy, family, home and correspondence, and protection of honour and reputation*, "provides for the right of every person to be protected against arbitrary or unlawful interference with his privacy."[2]

Most countries enshrine some form of privacy rights in their Constitutions. A compendium of information regarding the legal status of privacy and other civil rights around the world is maintained on the Human Rights Watch web site[3].

In the United States, the *First* (freedom of expression) and *Fourth* (security against unreasonable searches and seizures) *Amendments to the Constitution* are usually regarded as the essential legal principles that restrict the ability of the Federal government and other bodies (including law enforcement agencies) to gather personal information and communications without reasonable cause. *Fifth Amendment* rights – the protection against self-incrimination - are also at times invoked.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

In Canada, the Constitution Act of 1982 incorporated the *Charter of Rights and Freedoms*, which expresses the fundamental right of all people to "freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication"[4]. Extending these points, the *Privacy Act* (revised in 1985)[5] and the *Personal Information Protection and Electronic Documents Act* of 2000 [6] clarify public and private sector responsibilities regarding privacy, which the Canadian Supreme Court has called the "most important value… grounded on physical and moral autonomy…at the heart of liberty in a democratic state".

Why should we worry about our governments?

Internet intrusions on privacy by the commercial sector (in such forms as web cookies, spyware, web bugs, etc.) are not only relatively well-known to the technologically-aware public, but also the topic of seemingly endless discussion. Government intrusions, however, only seem to break through to the public consciousness at times of crisis; moreover, whereas the former are the subject of near-universal disdain, governmental encroachments are viewed in a far more equivocal light, often seen as “for our own good” or “in the interests of public safety”.

But governmental intrusions have unique and frightening qualities:

- unparalleled technical and legal resources that can brought to bear against users, marketers and developers of, for example, encryption ;
- the secret nature of their own anti-privacy projects;
- the lack of recourse afforded to their targets

As to the weight governments can bring, one of the well-known stories in this field is that of the plight of Phil Zimmerman, the developer of Pretty Good Privacy (PGP). For three years Zimmerman was the subject of a federal investigation – by posting a copy of PGP on USENET, he was alleged to have violated the State Department's International Traffic in Arms Regulations (ITAR), rules that classified strong encryption as "munitions" and therefore subject to export control. Zimmerman faced the possibility of five years in prison and a $1 million dollar fine. In the end, the Justice department declined to press charges. Zimmerman remains a passionate exponent of the social value of encryption – as he says, "If privacy is outlawed, only outlaws will have privacy."

Why does the U.S. government want to restrict encryption?

Simply put, encryption allows users to encode information so that access to a secret key is required for decoding. Widely available "strong" encryption can allow users to determine just what they wish to reveal to others. Unfortunately, some governments view this technology as improperly empowering their citizens. While encryption can be – and is – used by criminals, terrorists, etc., it is also a tool used by ordinary people with legitimate desires for privacy.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Security holes - "backdoors" – can be created accidentally or purposefully in encryption software. The FBI and other investigative agencies have attempted to convince Congress that intentional backdoors should be implemented in all such software in order to allow access to encrypted communications or files. Under most of these plans, a court order would be required to access the "key escrow" and retrieve the key needed to decrypt the information.

Even given proper intent, this is a dangerous concept. Note that a 1996 Presidential Commission on encryption policy contains a warning by the National Research Council: "Escrowed encryption by design introduces a system weakness… if the procedures that protect against improper use of that access somehow fail, information is left unprotected" (quoted in *The Risks Of Key Recovery, Key Escrow, and Trusted Third-Party Encryption*[7], a 1998 report by an ad-hoc group of eminent experts in cryptography and computer science, to which the reader is referred for an in-depth discussion of this issue).

Why should we be concerned about technology's role?

It might be tempting to regard technology as "just another tool" that governments or other bodies can employ to potentially erode our rights.

Marc Rotenberg of the Electronic Privacy Information Center (EPIC), however, has written compellingly of the need to focus particular attention on the complex relationship between surveillance and technology due to specific characteristics of the latter. Rotenberg notes how attributes such as *amplifictaion* (technology's ability to extend information-gathering capabilities), *routinization* (the process of normalizing intrusions into private lives) and *sublimation* (the mechanisms by which surveillance technologies become increasingly difficult to detect) threaten our rights in new and intricate ways: "While technology is not required for an invasion of privacy, the ability to amplify, routinize and sublimate surveillance has traditionally raised some of the greatest privacy concerns." [8]

Some recent milestones in governments' use of technology to erode the right to privacy.

The U.S. Federal government has always been quick to pick up on the use of technology to spy on communications. Stymied by legal restrictions on mail interception, the government began its first series of telephone taps in 1885, only four years after the introduction of the telephone in the country.

But to return to recent times…

While export of certain encryption technologies was long restricted under the International Traffic in Arms Regulations, it was the Clinton administration's championing of the Clipper chip and its insistence on 3rd-party escrow for all keys (which would have at one point included your bank card PIN) that brought the issue to the fore. Fortunately, there was enough opposition to all three versions of the Clipper plan to derail the proposals.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

The Security and Freedom through Encryption (SAFE) Act was originally designed to remove most limits on encryption use and export, as well as to prevent Clipper-like schemes in the future, but it was effectively gutted by FBI supporters in the legislature.

The Communications Assistance for Law Enforcement Act (CALEA) of 1994 requires telecommunications companies to modify their equipment, making it easier for government investigators to tap into private communications.

The FBI's infamous Carnivore system – belatedly renamed to the less imposing DCS1000 – is designed to monitor ISP traffic. It reads email headers (for now) and can report on http and ftp traffic as well. At the moment, its use still requires a court order.

And then there's ECHELON[9], the NSA-designed massive communications interception network. Its very existence is still officially denied by the U.S. and Canada, although the three other partners in the system – Great Britain, Australia, New Zealand – have all admitted their involvement. James Bamford notes "The real issue [for Europe] is… whether Echelon is doing away with individual privacy - a basic human right… Unchecked, [Echelon's] worldwide eavesdropping network could become a sort of cyber secret police, without courts, juries, or the right to a defense."[10]

Speaking of Great Britain – not only are the English the most watched people on the planet (more public CCTV cameras per capita than any other country, car license detectors in London, retinal scanners at Heathrow), but the Labour government's Regulation of Investigatory Powers (RIP) Act of 2000 established their right to peruse all internet traffic within the country. This effort is overseen by a department with a deliciously-Orwellian name: the Office of Technical Assistance.

What has happened since September 11th 2001?

Times were not looking particularly good for civil libertarians even before the tragedy. For example, only a week before the terrorist attacks, Ronald Dick, the Director of the National Infrastructure Protection Center (NIPC), stated that while "Americans have always recognized privacy as among the most fundamental of all human rights… [however,] the balance described in the Constitution… is eroding. In its place, the privacy of criminals and foreign enemies is edging towards the absolute."[11]

Even staunch privacy advocates seem to accept that new legislation and powers that specifically target terrorists may be needed in the aftermath of the September 11th attacks. However, it seems that in the U.S. and elsewhere a whirlwind of new and re-treaded proposals are being quickly passed into law with little if any debate.

The USA Patriot Act was signed into law in October 2001. This very broad legislation expands the application of CALEA to all electronic communications and effectively allows any member of the executive branch to conduct Carnivore-like surveillance. It even enables courts to allow into evidence information gained from illegal wiretaps.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Chilling effects? Immediately after the attack, Len Sassaman, the operator of a well-known anonymous remailer, suspended activity with this apology: "[I] don't have the resources to defend myself. At this point in time, a free-speech argument will not gain much sympathy with the Feds, judges, and general public." And a poll showed that 72 percent of Americans were in favor of some form of new anti-encryption law; Republican senator Judd Gregg of New Hampshire began drafting legislation that could revive the Clipper chip debate.[12]

In Canada the Anti-Terrorism Act was rushed through Parliament to quickly extend the powers of the federal government. It has an extraordinarily broad sweep, amending the Criminal Code of Canada, the Official Secrets Act, The Canada Evidence Act, the Canadian Human Rights Act, the Immigration Act, the Proceeds of Crime Act, Access to Information Act and others. Unlike its American counterpart, it contains no meaningful sunset provisions, despite its introduction as a temporary measure to fight the current terrorist threat.

In November 2001, MSNBC broke a story about Magic Lantern, part of the FBI's plan to enhance Carnivore. Magic Lantern is essentially a virus capable of keytrapping, designed to provide the FBI with encryption keys on infected victims' computers.[13]

Within the legal system, a ruling in January 2002 has perhaps opened the door to Magic Lantern or similar systems. FBI agents armed with a court order planted a keytrapping device in the computer of an alleged mobster and recorded his PGP encryption key. A federal judge rejected arguments that the FBI violated wiretap laws or Fourth Amendment protection.

In Europe the reactions have been mixed. One the one hand France is apparently re-thinking its recent decision to eliminate the requirement for 3rd-party key escrow. On the other, the European Parliament ignored a request from President Bush and passed a EU Directive on enhanced protection of privacy in the electronic communications – Bush had sought a number of changes in the proposal to allow for data retention of telephone calls and internet messages.[14]

What to do?

This paper has addressed some ways in which governments have attempted to use specific technologies to deprive people of their right to privacy. Technology, though, can of course also be used to protect, enhance and extend our individual liberties. It is our responsibility as citizens to act and vote in ways that ensure this comes to pass.

In particular, some things we can do include:

- Educating ourselves about these issues and our governments' actions.
- Affirming our support of fundamental legal rights to privacy and other civil liberties.
- Using technology to extend these rights.
- Shaking our heads in pity should we run into Scott ("You have zero privacy anyway…Get over it."") McNealy.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Finally, here are some organizations devoted to liberties and privacy rights (with an electronic communications bent) that the reader may wish to investigate:

- Electronic Privacy Information Center (EPIC). http://www.epic.org
- Global Internet Liberty Campaign (GLIC). http://www.glic.org
- Privacy International (PI). http://www.privacyinternational.org

References:

[1] United Nations. "Universal Declaration of Human Rights."
URL: http://www.unhchr.ch/udhr/lang/eng.htm (21 Jan 2002).

[2] UN Office of the High Commissioner for Human Rights. "The right to respect of privacy, family, home and correspondence, and protection of honour and reputation –General Comment 16." URL: http://www.unhchr.ch/tbs/doc.nsf/(symbol)/CCPR+General+comment+16.En?OpenDocument (21 Jan 2002).

[3] Human Rights Watch. "Freedom of Expression on the Internet."
URL: http://www.hrw.org/wr2k/Issues-04.htm (21 Jan 2002).

[4] Government of Canada. "Charter of Rights and Freedoms."
URL: http:// laws.justice.gc.ca/en/const/annex_e.html#I (21 Jan 2002).

[5] Government of Canada. "Privacy Act."
URL: http://laws.justice.gc.ca/en/P-21/81499.html (21 Jan 2002).

[6] Government of Canada. "Personal Information Protection and Electronic Documents Act."
URL: http://laws.justice.gc.ca/en/P-8.6/79806.html (21 Jan 2002).

[7] Ablson, Hal et al. "The Risks Of Key Recovery, Key Escrow, and Trusted Third-Party Encryption." URL: http://www.cdt.org/crypto/risks98/

[8] Rotenberg, Marc. "Preserving Privacy in the Information Society."
URL: http://www.unesco.org/webworld/infoethics_2/eng/papers/paper_10.htm (21 Jan 2002).

[9] Bernal, Javier. "Big Brother is On-line: Public and Private Security in the Internet."
URL: http://drecho.org/comunidad/echelon (21 Jan 2002).

[10] Bamford, James. Body of Secrets. New York: Doubleday, 2001.

[11] Dick, Ronald L. "The Legal Aspects of Infrastructure Protection." 5 Sep 2001.
URL: http://www.nipc.gov/pressroom/pressrel/090501.pdf (21 Jan 2002).

[12] Koerner, Brendan. " Technology and Its Discontents." Village Voice September 26 - October 2, 2001. URL: http://www.villagevoice.com/issues/0139/koerner.php (21 Jan 2002).

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

[13] Sullivan, Bob. "FBI software cracks encryption wall." 20 Nov 2001.
URL: http://www.msnbc.com/news/660096.asp?0na=x21017M32 (21 Jan 2002).

[14] Meller, Paul. " European Union Set to Vote on Data Law." New York Times ,13 Nov 2001.
URL: http://www.nytimes.com/2001/11/13/technology/13NET.html (21 Jan 2002).

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: June 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**