TRANSNATIONAL CYBERCRIME
October 12, 2010
by Elizabeth Hall

- Recommended book: Cyberwar: The Next Threat to National Security and What to Do About It by Richard Clarke. Ecco, 2010, 304 pages.

Cybercrime can be institutional or a rogue manipulation of privacy by individual hackers. Cyberwar uses the internet to invade private systems. Therefore, says Richard Clarke, the government should have to right to monitor all internet traffic to thwart cybercriminals. The Patriot Act already permits the government to monitor phone traffic in search of terrorists. The 4th Amendment to the Constitution would seem to protect personal privacy.

Vote taken: Should the U.S. government be allowed to monitor all internet traffic to protect us from terrorists? YES 11; NO 14.

YES: If hackers can already get anything they want, we delude ourselves in thinking we can escape monitoring. We're already there.

What is more important? National Security or Personal Security?

You can't restrict monitoring to National Security. When evaluating the question, consider that the government has excelled in presenting its own version of the truth—which may not be true. How do you choose between the two? Think long and hard before you allow the government to violate the 4th amendment.

Monitoring the internet is not to protect privacy, but to protect our way of life.

The 4th Amendment is also meant to protect political dissent. We see the results of lack of privacy in other countries. Who is monitoring our national security? Consider some of the candidates for office today. Would you like them to be invading your privacy?

Who is national security? Who is homeland security? Our computers are already monitored. We need a way to determine who is doing it. We're naïve and vulnerable. Monitoring exceeds the requirement for national security.

You can make a conscious choice not to participate. No e-mail, no internet, etc. Do you think you can really disengage? Credit cards, social security numbers, already leave you engaged. You can focus on limiting vulnerability through computers. But it's not ideal

American are already willing to give up privacy on Facebook and Twitter. So there's unlikely to be much alarm at the monitoring. To what extent does the current "twittering" generation object to it? Some people who object to monitoring have been using credit cards for years.

We can become aware of our own vulnerabilities. Educate ourselves about phishing. When BOCES agreed to remove social security numbers that were not encrypted, it took them a year to find another way to track people. You have to give your social security number when you donate blood; FDA needs to be able to track bloodsources. Washington DC's voting machines had to be pulled, because the system passwords were unsecured. There's no law against businesses storing personal information in unsecured files. Most transactions require you to read and click that you have done so—and the agreements protect businesses.

Would you insert the word "unconditional" in the original question?

So if there are enough checks and balances, it's okay for the government to monitor the internet? Who guards the guardians? We don't know what we don't know. Would there be congressional oversight with revelations to the public? How can you defend yourself? If you cannot have confidence in the "guardians," we're deeper in the soup than we thought.

With tracking married to your credit card, the genie is already out of the bottle. Many people are unaware what sites like Google and Facebook are doing. Should this country be made aware of the current level of eavesdropping? Facebook has intruded so far beyond what we're prepared to define as personal privacy. If we knew the level of privacy we've already lost, there would be a major uproar. Our cars, phones now possess gps devices. We can all be tracked. The ability to get information through the computer is incredible. People should be licensed to use computers. But a lot of the monitoring is being done by institutions, corporations, etc.

The conflict between authority and freedom is always present. There's no black-and-white answer, but some kind of agreed-on balance.

It's just good luck that the Times Square bomber was unsuccessful. What if the government issued regular reports that x number of attempts were forestalled by internet monitoring? But who do you trust to give you a credible report?

The assumption is that there's a relation between increased security and loss of privacy. But there may not be a connection. The fear in this country is of a single terrorist incident. But we can't eliminate possibilities.

Are there alternate ways that could avoid monitoring? How about making computers more secure?

Have we created a body of law that gives us a right to privacy?

Part of our problem is that everything is "all." We need to use "some." We do need a C.I.A., an F.B.I. Today neither is accountable. Where is there any watching of the watchers?

Many sources are no longer reliable. Photoshop can change any photo. Corporations can write their own Wikipedia articles.

It's an illusion that giving up privacy would gain us more security. It's the wrong question. Smaller questions may be more important. Consider the problem of identity theft. There are somethings the government can do. For example, the failure of businesses to protect privacy by encryption should be a crime.

Vote taken at the end of discussion:
Should the U.S. government be allowed to monitor all internet traffic to protect us from terrorists?

YES: 9; NO 15

See attached definitions of "privacy"

Definitions of “privacy”

pri·va·cy (prī′və-sē)
n. **1. a.** The quality or condition of being secluded from the presence or view of others.
b. The state of being free from unsanctioned intrusion: *a person's right to privacy.*
2. The state of being concealed; secrecy.

The American Heritage® Dictionary of the English Language, Fourth Edition copyright ©2000 by Houghton Mifflin Company. Updated in 2009. Published by Houghton Mifflin Company. All rights reserved.

Privacy [ˈpraɪvəsɪ ˈprɪvəsɪ]

n **1.** the condition of being private or withdrawn; seclusion. **2.** the condition of being secret; secrecy.**3.** (Philosophy) *Philosophy* the condition of being necessarily restricted to a single person

Collins English Dictionary – Complete and Unabridged © HarperCollins Publishers 1991, 1994, 1998, 2000, 2003

ThesaurusLegend: Synonyms Related Words Antonyms

Noun 1. privacy - the quality of being secluded from the presence or view of others

seclusion, privateness

reclusiveness - a disposition to prefer seclusion or isolation

2. privacy - the condition of being concealed or hidden

concealment, privateness, secrecy

isolation - a state of separation between persons or groups

covertness, hiddenness - the state of being covert and hidden

bosom - the chest considered as the place where secret thoughts are kept; "his bosom was bursting with the secret"

confidentiality - the state of being secret; "you must respect the confidentiality of your client's communications"

hiding - the state of being hidden; "he went into hiding"

Based on WordNet 3.0, Farlex clipart collection. © 2003-2008 Princeton University, Farlex Inc.