GlobalResearch
Center for Research on Globalization

Digital Data and the Loss of Privacy

By Global Research News
Global Research, June 17, 2015
BATR 16 June 2015

Region: USA
Theme: Intelligence

The tech culture would have you believe that the digital format has produced untold innovations and advancements for personal development, societal advancement and business innovations. Well, the glass is half full for the kool aide drinkers, but for the mere mortals, who seek out a meaningful life as opposed to a regimented existence, the curse of placing the most intimate data on untold hard drives and shuffled among unknown servers, a loss of simple privacy is the least of the problems.

The horror of keeping the door unlocked to the treasure chest of government and business secrets seems not to faze the computer gurus who pushed for decades that going digital was the holy grail of efficiency and productivity. Encryption was the answer to securing central databases of zeros and ones that store the most desirable information of national security.

When the mainstream USA Today warns, The hacking of OPM: Is it our cyber 9/11? – The cover-up of a vulnerability of unlimited sharing of data from security breaches should be a substantial alarm call.

> Although the announcement of the hacking into the computers of the OPM and the stealing of personal data on more than four million present and former federal employees was made in late May, the data breach had been discovered a month earlier and had been going on undiscovered for more than a year.
>
> An obvious question about this latest data breach is why were the hackers seeking this information and the answer at this time is that we do not know. This type of information could be used for purposes of identity theft for profit, for gathering information to be used by the Chinese government to enhance their spying capabilities or even as part of their ongoing worldwide corporate espionage efforts by which they steal corporate and military secrets, such as the theft of secret plans of our most advanced F-35 Stealth Fighter Jet which was accomplished by hacking into computers at the Pentagon and at Lockheed Martin, the builder of the plane. Evidence of the hacking of the F-35 was leaked to the public by NSA whistleblower Edward Snowden.
>
> In May of 2014, the Justice Department indicted five Chinese military personnel on charge of hacking into six American companies to steal corporate secrets, however this type of activity has gone on for years. According to security company Mandiant, Chinese hackers have stolen corporate secrets from 115 American companies since 2014 and it is not just the Chinese who do this type of corporate espionage. Russia has also been particularly active in corporate cybercrime. It was estimated by cybersecurity company CrowdStrike that the Russian government has hacked hundreds of companies around the world in order to steal trade secrets and corporate information they can exploit.

Now it should be self-evident that spying from friends or foes are normal occurrences in a hostile world. Citing the theft of design, confidential technological and engineering details, obviously should be of concern to all citizens. However, the pattern of hacking and easy access to such information just does not seem to rise to the highest national concern.

The question that is seldom asked is whether placing such sensitive secrets on networks that can be used by anyone, who can duplicate or pilfer the authorization credentials to login, is a core and systemic issue.

With all the billions spent on the computer spy game, one would reasonably wonder why keep in a digital format the most important information resources that seem to be the highest objective on the target list for foreign theft.

Espionage makes use of the most sophisticated methods for penetrating the barriers attempting to protect the information. Remember when the U.S. Embassy in the Soviet capital was penetrated with an eavesdropping device, the response was to communicate using an Etch-a-Sketch toy? Magic Slates don't blow up, go fast or even scare the dickens out of the bad guys, but the erasable memo pads nonetheless came in handy for two congressional delegates trying to outsmart spies during a mission to Moscow.

While this example used voice recording, the permanent horde of computerized data is a far more significant gold mine of information. The miracle of the computer revolution has turned into the nightmare of espionage extraction.

Consider how implausible it would be for a human spy to use a Minox camera from the cold war era to photograph top secret documents that were instantly transferred from the Chinese hack. Back in the "good old days" of low tech, organizations and bureaucracies stored their records on magnate tape drives in-house. Those vast sharing networks in cyberspace did not exist and the only cloud known was the one that carried the rain.

Today, the storm from relying on some exotic algorithm formula that claims to safely encrypt and secure any database is like placing your faith into the iPhone culture of assured communication. Back doors are the true entry gateway of global digital dissimulation.

Surrendering safekeeping for the promise of easy sharing, misses the entire purpose of why secrets in any business or government are kept in the custody and stewardship of trustworthy persons, managing systems of formidable barriers that resist theft and broadcasting.

What lessons were learned from Edward Snowden? For all the scorn dumped on this whistleblower, what was the method of his disclosures? The digital format of the files begs for accessing the data, for whatever motive the expert exhibits.

Even harsh critics of Snowden do not make the case that he was a foreign agent plant. However, just imagine the kind of damage that could be accomplished if an undercover spy had access to the type of databases that a civilian contractor at the NSA was able to transmit.

Centralizing critical information under firewall barriers has little guarantees that networks are secure. Since the digital format is the new standard, just maybe, going against the grain is the prudent method to keep real secrets, confidential.

Submitting the most important and sensitive to paper and not on computers might well supply a much safer policy than depending on security clearances to protect top secret documents.

Abandoning the old fashion tax reporting filings for an electronic submission is a formula for opening financial records on all tax payers. Surely, companies should get nervous over certain details that may not be part of public disclosures. And government technocrats should be put on notice that their role in protecting the system may just require their own agencies to be put under the microscope.

If whistleblowers were the main source of hacks, the risk might be relatively minimal. Conversely, falling under the state sponsored hacking initiative certainly has every aspect of an act of war. Certainly, the prospect for a heated up confirmation is unlikely for no other reason that it is reasonable to conclude that the U.S. is well skilled in its own espionage operations.

Nonetheless, it should be recognized that transparency is not defined as direct access to every database, both public and private.

Digital files are well appreciated for library archives, news reports and political debate, but when foreigners attack information platforms that are intended to secure personal disclosures, the outrage should be more intense and the press needs to feature the problem.

Privacy has become a dirty word for the collectivists who want to dominate individual behavior. Yet, the stuck on stupid crowd continues to voluntarily provide the most intimate details on their lives on every government form or in surveys.

The databases, themselves are the issue. A society that rushes to send “selfies” on the internet, is hardly a culture based upon prudent and protective privacy.

Accepting the digitalization of all information guarantees that the only security available rests upon non participation in the electronic communication environment. Even dropping out of the computer revolution will not retake your former disclosures.

Files, yes digital format, are so prevalent that only the unborn do not yet have a dossier on file.

It is one thing for Google, Facebook and Amazon to assemble personal profiles and project future behavior. But it is much worse for governments to target citizens of other countries for accumulating background information of civilians.

Lesson learned. There is no security in cyberspace.

If the information you want to protect is important, maintain the details in a privately secure paper format. By this definition, banking, employment, medical and educational circumstances are almost impossible to keep private.

As for national security secrets, will you not agree that this is one area where the government should scale back on network access databases that are so vulnerable to foreign infiltration and spying?

Let the debate be about expanding public disclosure on government policies and programs and keep the personal background data, private. If you believe that Net Neutrality regulations will provide greater security, the opposite will happen.
