Surveillance & Society

Opinion

Under-Explored Threats to Privacy: See-Through-Wall Technologies and Electro-Magnetic Radiations

Vanmala Hiranandani

Independent researcher, UK. Vanmala_hi@yahoo.com

Introduction

Protecting the privacy and security of personal information has gained increasing attention in recent decades, as a result of the proliferation of numerous surveillance technologies and information databases that have problematized the individual's right to privacy. Indeed, increasing surveillance and monitoring of personal information have become intrinsic characteristics of modern societies. While information collection and invasive surveillance technologies have multiplied rapidly in recent years particularly since September 11, legislation to protect individuals' privacy rights has lagged far behind. Consequently, while information enthusiasts loudly proclaim an era of perfect communication where "all information [exists] in all places at all times" (Poster 1990: 70), privacy advocates exhort us to think about the ramifications for civil liberties, privacy, and democracy itself. As a result, literature that analyzes the repercussions of surveillance technologies has increased extensively over the past two decades (see Lyon 2002a).

Furthermore, the recent months have seen increased news coverage about domestic spying in the USA (see e.g. Goodman and Gonzalez 2009) – spying that many individuals from minority groups have long suspected but have felt powerless to bring to mainstream attention. However, despite remarkable advances in surveillance studies and increasing news coverage on domestic spying, several significant gaps persist that merit further research and analysis. It is essential to point out two things: firstly, most existing literature and recent news items have been framed in general terms presuming that domestic surveillance is being exercised on everyone equally. The unequal consequences of surveillance techniques for certain sub-groups of the populations, such as racialized groups and new immigrants in USA, UK and Canada, have received insufficient attention; this seriously limits and under-informs public debate.

Secondly, reports on domestic surveillance in the US have been limited to wiretapping that includes surveillance of phone and email correspondence and internet monitoring. Likewise, in surveillance studies, Lyon's (2004) noteworthy synthesis cites examples that are limited to video images in public places, personal identification numbers, radio frequency identification (RFID) tags attached to merchandise by manufacturers to trace items, biometric recognition systems, and navigational systems and cell phones that use global positioning satellite (GPS) technology to trace location. Most surveillance research examines monitoring regimes in public places, overlooking technologies that can penetrate private spaces, such as homes. There has been little or no discussion on audio-bugging of homes and offices, or the use of little-known technologies that permit theft of offline data through electro-magnetic radiations (known as TEMPEST) and seeing through walls. The use of audio-bugs to record and monitor

Hiranandani, V. 2010. Under-Explored Threats to Privacy: See-Through-Wall Technologies and Electro-Magnetic Radiation. *Surveillance & Society* 8(1): 93-98.
http://www.surveillance-and-society.org | ISSN: 1477-7487

conversations is perhaps not new (see for example Budiansky 1987; Free, Freundlich and Gilmore 1987), yet their use on foreign visitors, international students and academic faculty, or those perceived to be subversive, to monitor conversations in their homes in the post-9/11 environment has been under-researched.

This paper chooses to focus on the two aforementioned technologies of electronic eavesdropping: capturing electro-magnetic radiations (EMR) from computer screens and using see-through-wall gadgets that have been hitherto hidden from public knowledge. While computer science, engineering, technology journals and news sources have shed light on these technologies, sociological and surveillance studies have remained far behind in their analysis of such surreptitious mechanisms. As such, privacy and human rights implications of these highly intrusive techniques continue to be largely unexplored by sociologists and surveillance scholars alike. The purpose of this paper, therefore, is to draw attention to these under-studied technologies and to underscore the need for greater investigation of these invasive gadgets as well as their repercussions for individual privacy that is at the core of human dignity and a civilized society.

Under-explored technologies – Electro-magnetic radiations (EMR/TEMPEST) and see-through-wall

EMR / TEMPEST:

In the 1950s, researchers became aware that computers generate electromagnetic radiations (EMR) that can easily be used to reconstruct information about the data being processed by the device emitting it (Kuhn and Anderson 1998; Zalud 2004). The term TEMPEST (Transient Electromagnetic Pulse Emanation Standard) originated from a classified EMR study conducted for the U.S. military in the 1960s and was initially used to indicate a set of practices designed to prevent leaking of emissions from electronic devices processing sensitive data (Wiegner, 1990; McCarthy, 2000). It later became a buzzword for denoting a general class of problems and techniques pertaining to the interception and reconstruction of radio frequency emissions.

Leaking of information through EMR emissions was first discussed publicly by Dutch computer researcher, Wim van Eck (1985), who confirmed that it is quite easy to reconstruct images and text displayed on computer monitors by intercepting radio frequency signals generated by high-voltage circuits inside such devices. This process of eavesdropping on the contents of CRT and LCD displays using its electromagnetic radiations came to be known as Van Eck phreaking, after its pioneering researcher.

Anyone reasonably skilled in monitoring radio frequencies and using a few thousand dollars of commercially available equipment can intercept and capture information from an offline personal computer from a radius of up to one mile (Wiegner 1990; Zalud 2004). The invisible, information-laden radio waves from a computer monitor, similar to a broadcast TV signal, `can be picked up by a spy's scanner and antennae tuned in to the waves, which can then be processed line by line to replicate the image on the original screen (McCarthy 2000). Thus, with modest equipment, an eavesdropper can construct a complete transcript of a victim's actions – every keystroke and piece of data viewed on the computer screen or sent to a printer can be hijacked, thereby compromising the security of passwords, personal and official messages, intellectual property etc. (Garfinkel 2001). Menzies (1998) explains how the Tempest/Van Eck System Monitor, costing about US$1,900, allows the hacker to remotely monitor computers, ATMs, TVs and all other displays using a TV or multisync monitor. The monitoring equipment can be powered by batteries, thereby making it portable. An eavesdropper can be seated in his car while viewing the victim's typing on their computer in their home or office. As Gehling, Ashley and Griffin (2007) caution, while most office buildings are designed to prevent physical intrusion, electronic surveillance enables eavesdroppers to intercept computer data and spy on meetings without entering an

organization's office space or building. This is a particularly nasty threat for information security because whatever is on the screen, even offline, can be transmitted to hackers and unscrupulous eavesdroppers.

Several years ago, the Dutch scientist, van Eck, approached the British Broadcasting Corporation (BBC) to film him while he used an antenna-equipped vehicle to snoop on computers inside several buildings in London. Of course, van Eck did not reveal any of the information he had gathered. His presentation, despite featuring on the BBC show, 'Tomorrow's World,' was seen as an oddity at a time when home and office computers were not as common (McCarthy 2000). Aside from a few scientists' demonstrations and van Eck's televised stunt in London in the 1980s, instances of this kind of computer surveillance have been hidden from public knowledge.

Eavesdropping by remote detection of electromagnetic signals from desktop and laptop computers, that today process everything from personal bank records to corporate secrets, is perhaps the most sinister type of information piracy. Thus far, information security concerns with regard to personal computers have generally been limited to data piracy via the internet and email correspondence (see for example Campbell and Carlson 2002; Lyon 2002b). Most computer users are worried about internet privacy in the digital age wondering who is reading their emails or watching the pages they view online. Apart from the common knowledge that computer monitor radiations cause headaches and eyestrain, most people know little or nothing about the radio-frequency waves emitted by their computer screens that can be isolated and captured with directional antenna focused on a computer or room from a nearby office, or a floor below or even across the street. Data can, thus, be thieved literally through thin air without even needing phone lines (McCarthy 2000). As McCarthy mentions, a letter, a sales proposal, an R & D report or a correspondence to a lawyer can all be captured from as far away as hundred yards, without the victim's awareness. Since each video screen's signal is unique, the eavesdropper can easily receive and decode the signal, leaving no avenue for the victim to be able to prove the information theft (Donlan 1986). Even the computer industry has only recently realized that most computer terminals and screens radiate emanations that are strong enough for a sensitive receiver to decipher the screen's contents even when the computer is not connected to the internet (Lehtinen and Gangemi 2006; Zalud 2004). Although emanation leaks comprise an important field of research from ethical, legal and sociological standpoints, they have been mostly unexplored in the fields of law, social sciences and public policy.

U.S. military and intelligence agencies have been concerned about what they call 'compromising emanations' from computers (Donlan 1986; McCarthy 2000; Zalud 2004). McCarthy (2000) informs that some US government agencies and defense contractors use shielding technology known as "TEMPEST" that sets certain standards in the design of computer monitors and network cabling to contain emissions of electromagnetic signals. A covert industry has quietly emerged to market shielding equipment; however, interestingly, selling protective paraphernalia requires government licensing. McCarthy further mentions that the National Security Agency lists eighteen companies on its website whose computer equipment meets government standards of electromagnetic emanations. However, overall, relatively few U.S. companies outside of defense-contractor networks appear to be knowledgeable about the possibilities of computer-monitor surveillance or the US government's TEMPEST program.

The legal implications of spying on someone's computer monitor from a distance are yet unclear and murky since courts have yet to examine this issue. There is no US federal law to oversee computer surveillance through electromagnetic radiations. Although states have widely ranging anti-eavesdropping laws, consideration of the theft of data through the air has been lacking. While laws exist to protect the privacy of communications, legal scholars argue that typing to oneself is not communication, which requires correspondence between two or more persons or entities (McCarthy 2000; Wiegner 1990). Although the legal arena has yet to engage in extensive debate on this issue, eavesdropping and theft of data from computer screens is undoubtedly unethical and abhorrent. It goes without saying that the

possibility of plagiarism and copyrights violations using this type of insidious and devious computer eavesdropping has received no attention.

Through-wall surveillance (TWS):

Even more intriguing is the invention of equipment to see through walls, such as infra-red cameras, thermal imaging, and through-the-wall surveillance technologies that can detect activities behind walls and in darkness, thereby providing information on the location and movement of people inside buildings and homes (Bush 2006; Hunt, Tillery and Wild 2001; Miles 2007). Through-the-wall radar devices, which are lightweight, portable and able to focus up to twenty or thirty meters ahead, are increasingly available to municipalities and law enforcement agencies (Jones 2005). RadarVision, built by Time Domain Corp. of Huntsville, Alabama, and Prism 100 made by Cambridge Consultants Ltd. in Cambridge, England can detect the presence of inanimate objects through the wall, but only moving objects (in the form of a moving blob of color on their built-in color screens) are shown to the user. The product – for use by emergency and security services – weighs about six pounds including a lithium-ion battery pack. Since both these devices can be used from outside a residence or an office, such as from a neighboring home or building, they pose a challenge for targeted persons to know and prove that they are being monitored (Jones 2005).

Researchers at Atlanta's Georgia Technical Research Institute have made a flashlight that can see through doors and walls, thereby detecting a stationary person's presence through solid wood or an eight-inch block wall from four feet away (Sanders 2001). The flashlight uses simple microwave technology. It emits an invisible beam of electromagnetic radiation similar to automatic door sensors that sense movement. A commercial version is no larger than a police flashlight and costs less than $500 (Scott 1997).

Little is known about the government's hushed Celldar project that originated in Britain in 2002. The Celldar uses radar technology to allow surveillance of anyone, at any time, and any place where there is a phone signal. It uses mobile phone masts to allow authorities to watch vehicles and individuals almost anywhere. A report published in Britain's newspaper *The Guardian* mentions that this equipment has 'X-ray vision' potential – the capability to see through walls and look into people's homes (Burke and Warren 2002).

Although through-the-wall-surveillance (TWS) technologies are touted as life-saving measures (see Miles 2007), the secrecy of these gadgets and their introduction without widespread public consultation or judicial oversight increases the likelihood of their misuse. While these technologies are mainly available only to military and law enforcement agencies, to date there is no legislation regulating their use or ensuring transparency or accountability on the part of those entrusted to use these devices for emergency, crime prevention and disaster relief purposes.

Both through-the-wall surveillance and computer monitoring using electro-magnetic radiations provide an unfair advantage to the snooper and raise a variety of troubling issues including intrusion, searching without warrant, denial of due process, absence of informed consent, deception, manipulation, errors, possibility of targeted harassment, misuse of private property, and lessened autonomy. Besides, there have been no investigations on the health consequences of these surveillance gadgets for the watcher and the watched. In the prevailing psychosis of fear, xenophobia and fear-mongering, the surreptitious use of these technologies in a snitch culture leaves little possibility to provide evidence of reprehensible privacy violations. Thus far, only one study (Nunn 2001) has called for critical analysis of these military and police technologies that are increasingly being used in urban areas in the name of 'public safety'. As these technologies diffuse into the population, Nunn exhorts many questions must be answered about the privacy impacts of these devices, their effects on the everyday life of civilians (and one might add, on the sanctity of the home), as well as the legal implications of profiling technologies.

With these unprecedented invasive technologies, barriers and boundaries – such as distance, darkness, walls, curtains, doors and windows – that have been basic to our conceptions of privacy and human dignity are compromised. Given the significance of privacy for a democratic and civilized society, this essay makes an urgent plea for more investigation on the consequences of new surveillance technologies for various sub-groups of the population as well as increased public education about the cornerstone of all civil rights called privacy. Over-enthusiasm and infatuation with technological 'progress' and gimmickry can obscure the real dangers of the repressive potential of these so-called technological innovations, leading to a tyrannical, totalitarian society and harassment of those perceived to be subversive. It is imperative to demand transparency from those whose power is enhanced by technologies that render homes, buildings and individual lives transparent. Indeed, democratic civilian control of law-enforcement and security agencies and education about information piracy through unconventional means is crucial and central in the struggle to protect and extend democratic rights (see Caparini and Cole 2008). Rather than limiting the discussion of contemporary surveillance to individual privacy, we must redefine surveillance in terms of institutional accountability that "acknowledges surveillance as a structural problem of political power" (Stalder 2002: 123).

Concluding remarks

This paper has emphasized that while research and literature on surveillance and society has burgeoned in recent decades, several invasive technologies, such as electromagnetic radiations (EMR) and through-the-wall surveillance (TWS) mechanisms, as well as their privacy and health implications for the common public continue to be unexplored. The post-9/11 policy trend seems to be towards capitalizing on fear while hushing the intrusive nature of surveillance and information-gathering technologies (Samuel 2003). Legislation to protect privacy and civil liberties, already inadequate, has been substantially weakened in the post-9/11 era (Lyon 2001), while the use of surveillance techniques has multiplied legally and illegally, constitutionally and unconstitutionally, ethically and unethically. Therefore, this essay has argued for greater vigilance through future research, public education, and demand for government and police accountability about stealthy technologies that can invade privacy in unprecedented ways with little or no public awareness.

Establishing accountability measures for handling personal information and bringing to book those who abuse their power with unchecked surveillance is vital for the survival of democratic societies. It is imperative not just to oppose inhuman forms of physical torture in contemporary times, but also to prevent supposedly benign, perhaps more widespread forms of secret techniques shrouded in 'security' justifications, particularly in an Orwellian era when human rights and privacy concerns have taken a backseat. Privacy is at the core of human dignity, and its violation is nothing short of dehumanizing psychological torture.

References

Budiansky, Stephen. 1987. "Cheaper Electronics Make it a Snap to Snoop." *USA News & World Report*, May 18, pp. 54-56.

Burke, Jason and Peter Warren. 2002. "How Mobile Phones Let Spies See our Every Move." *The Observer*, October 13. Retrieved April 3, 2006 (http://observer.guardian.co.uk/uk_news/story/0,6903,811027,00.html)

Bush, Steve. 2006. "Police will use radar to see through walls". *Electronics Weekly*, November 17. Retrieved February 2, 2008 (http://www.electronicsweekly.com/Articles/2006/11/17/40181/Police+will+use+radar+to+see+through+walls.htm)

Campbell, John and Matt Carlson. 2002. "Panopticon.com: Online Surveillance and the Commodification of Privacy." *Journal of Broadcasting and Electronic Media* 46: 586-606.

Caparini, Marina and Eden Cole. 2008. "The Case for Public Oversight of the Security Sector: Concepts and Strategies." In Eden Cole, Kerstin Eppert and Katrin Kinzelbach, eds., *Public Oversight of the Security Sector: A Handbook for Civil Society Organizations*. New York: United Nations Development Program, pp. 11-30. Retrieved March 20, 2009 (http://europeandcis.undp.org/home/show/D090FFB5-F203-1EE9-B03268DF463A4CEE)

Donlan, Thomas. 1986. "No Tempest in a Teapot." *Barron's National Business and Financial Weekly* 66(39): 14, 53.

Free, John, Naomi Freundlich, and C. P. Gilmore. 1987. "Bugging." *Popular Science,* August, 231, pp. cover-9.

Garfinkel, Simson. 2001. *Web Security, Privacy and Commerce*. Sebastopol, CA: O'Reilly.
Gehling, Robert, Ryan Ashley and Thomas Griffin. 2007. "Electronic Emissions Security: Danger in the Air." *Information Systems Management* 24(4): 305-310.
Goodman, Amy and Juan Gonzalez. 2009. "Obama Administration Claims 'Sovereign Immunity' in Attempt to Dismiss Lawsuit Against NSA Over Domestic Surveillance." *Democracy Now!* April 19. Retrieved April 20, 2009 (http://www.democracynow.org/2009/4/16/obama_faces_deadline_today_over_release#)
Hunt, Allen, Chris Tillery and Norbert Wild. 2001. "Through-the-wall Surveillance Technologies." *Corrections Today* 63(4): 132.
Jones, Willie. 2005. "No Place to Hide: Portable Radar Devices See Through Walls and Report What's Inside." *IEEE Spectrum Online*. Retrieved February 2, 2008 (http://www.spectrum.ieee.org/nov05/2146)
Kuhn, Markus and Ross Anderson. 1998. "Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations. Retrieved February 4, 2008 (http://groups.csail.mit.edu/cis/crypto/classes/6.857/papers/ih98-tempest.pdf)
Lehtinen, Rick and G. T. Gangemi, Sr. 2006. *Computer Security Basics*. Sebastopol, CA: O'Reilly.
Lyon, David. 2001. "Surveillance after September 11." *Sociological Research Online* 6(3). Retrieved November 16, 2008 (http://www.socresonline.org.uk/6/3/lyon.html)