Virtual Borders and Surveillance in the Digital Age: Visit-US

Professor David R. Burns
Southern Illinois University
mayaprof@yahoo.com

Introduction

Several recent developments concerning technology and humankind have changed the way borders are being designed. In this paper, I have categorized what I see as the three major tiers of developments: global monitoring, ubiquitous computing technology and the pervasive use of biometrics to create virtual borders.

Tier I: Global monitoring

Nations have been active in monitoring global communications for some time, but Echelon is the most comprehensive system that has been exposed to the world's citizenry. Echelon is a global network of listening stations and satellites that monitors all forms of electronic communications that cross borders: land and cellular phone calls, faxes, e-mail and radio signals are monitored, recorded and cross-referenced as they move through and across international borders.

Echelon was forged by a clandestine Anglo-alliance between the United States, Canada, Australia, New Zealand and Britain in 1948. Initially, the program was an agreement between the US and Britain to operate sensitive listening posts that were capable of monitoring international communications. By allowing Canada, Australia and New Zealand into the program, the US and Britain were able to cast a very wide net; Echelon was capable of picking up and monitoring worldwide communications from Europe, Africa, Asia, Australia, North America and South America. As part of the program, each of the Echelon member's intelligence agencies were charged with monitoring and gathering global communications (Port and Resch 1999: 10-11).

In 1999, the Echelon program began gaining critical media attention. On 31 May 1999, *Business Week* published an article describing the history and direction of Echelon's surveillance. Comparing the program to the arrival of Big Brother, the article explained how supercomputers are capable of monitoring global communications, automatically filtering individuals' communications, and listening for keywords. If certain strings of keywords are picked up, the data is sent to human analysts for further review (Port and Resch 1999: 10-11). There was also media concern about the United States using Echelon for purposes other than security. *The Houston Chronicle* detailed a European probe of the United States' use of the Echelon program. European parliamentarians charged that the United States was using the Echelon program to help American companies compete unfairly in international competition for commercial contracts (Pasqua 2000: 18).

These articles indicated a shift from the US government's physical control and physical monitoring of individuals to its virtual control and surveillance of individuals. In the classic Foucauldian model of control and discipline, if someone or some entity needed access to an individual's communications, a human, localized, physical authority such as a judge could grant permission vis-à-vis a search warrant for a physical inspection of the individual's physical communications records in a physical location (Foucault 1977: 77-78). When the US and its allies adopted the Echelon program, there was a shift to the virtual control and monitoring of individuals. With the use of listening posts, satellites, digital networks and supercomputers to monitor phone calls and emails. The old model of local physical controls over individuals' communications within and outside of physical borders broke down and was replaced by a digital decentralized apparatus of control that transcended physical borders.

Tier II: Ubiquitous computing technology

A second area of note involves GPS chipsets and WIFI technology. Some governments' justification for the mandatory installation of GPS chipsets in cell phones is that this technology allows emergency and police teams to monitor and track down a subject's location more easily (World Press Review 1999). Again, a noticeable shift away from controlling an individual's static, physical address to controlling and monitoring an individual's mobile dynamic address through the use of digital technologies.

In fact, there may come a time when an individual is no longer seen as a fixed target within his postal code's physical border. With the pervasive use of GPS and WIFI technologies, people may find that shops they pass will send electronic promotions to their cell phones or PDAs to lure them into these shops' interior borders. One of the best illustrations of this is the scene in *Minority Report* (2002) where a number of storefronts directly market to the main character, Officer Anderton, as his physical location shifts in real time. Officer Anderton is tracked, targeted and solicited by biometric scanners that read his eyes. The same type of system could be applied to an individual driving his car within and across physical and virtual borders. More and more new cars are being bundled with pre-installed GPS or satellite technologies such as OnStar and satellite radio. With these technologies, both cars and their drivers can be monitored.

With the technology described above, individuals could still opt out of owning cell phones or installing the latest technological gizmos on their PDAs or their cars. It is the technological component in their consumer items that are being tracked across physical and virtual borders. The individual in his organic form is less relevant. He is just the transportation mechanism for a digital, ubiquitous transmission and tracking system.

Tier III: Biometrics and virtual borders

Currently, there is another shift underway in how people are being monitored and controlled as they move within and across borders. This shift is away from using external identifiers such as cellular phones and vehicles to using almost invisible, localized, organic biometric identifiers. The US Department of Homeland Security (USDHS 2004) defines biometrics as measurable physical characteristics 'used to recognize the identity or verify the claimed identity of an enrollee. Among the features that can be measured are face, finger scans, hand geometry, handwriting, iris, retina, vein, and voice'. It is this emerging area of research and development that will have the most pervasive and profound impact on the future of personal information and personal movement; it is where the organic and the virtual will collide in a seamless manner. Ultimately, I envision a ubiquitous, seamless model of surveillance and control that extends beyond physical borders.

The most recent and large-scale example of this effort to monitor and control individuals' movements within and across borders using biometric identifiers is called the US-Visit program. Since January 2004, US-Visit entry procedures were operational at 115 airports and 14 seaports (Department of Homeland Security 2004). The US-Visit program is not restricted to US soil. According to the USDHS (2004), US-Visit is a security program that is initiated overseas when a person applies for a visa to travel to the United States. This security program 'continues on through entry and exit at US airports and seaports and eventually, at land border crossings'. The USDHS (2004) explains that the 'US-Visit program enhances the security of US citizens and visitors by matching the identity of visitors with their travel documents'. According to the USDHS (2004), this security program 'facilitates legitimate travel and trade by leveraging technology and the evolving use of biometrics to expedite processing' at US borders. Overseas US consular offices take biometric data from visitors using digital finger-scans and photographs. This biometric data is checked against suspected terrorists before a visa can be issued. When a visitor arrives at a US border, that visitor's biometric information is collected again and matched against a database to verify the visa holder's identity (Department of Homeland Security 2004).

Since August 2007, US citizens applying for or renewing their passports have been issued e-passports that contain chips that store personal and biometric data. Older US passports without the chips will be valid until their expiry period (USDS 2008). These policy changes indicate a clear shift in US internal policy away from a disciplined society to a controlled society. In a disciplined society, US citizens would follow laws regarding presenting

documentation to enter and exit borders. However, the USDHS seems to want to shift away from a disciplined society towards a controlled society. US citizens who comply with biometric sampling (e-passports) will have their biometric data filtered through a controlled system allowing rapid border crossing via an apparatus of digital controls.

Who ultimately has access to the personal information being collected? The USDHS website reports that the system is available to appropriate US federal, state and local agencies. How far away are we from a system being used to profile, index, track and monitor citizens? In the past, the USDHS required that airlines and cruise companies report personal passengers' information to them. If this information is combined with individuals' credit card information, a complete profile becomes clear. Companies like Acxiom collect individuals' contact information, estimated incomes, home values, occupations, religions, shopping habits and keep records for TransUnion, one of the world's largest credit reporting agencies. All of this type of information has been shared with the US government since 9/11 (O' Harrow 2005: 36-37).

The tiers of surveillance developments described above range from government satellites, which monitor personal communications, to cell phones, which allow for the observation of an individual's physical location, to virtual border controls. Thinking of Orwell's *1984* (1977), one wonders whether such an all encompassing data gathering system could or would be used to profile, index and track citizens' movements both physically and virtually. How is it currently being used to track citizens' movements locally, globally, and dynamically? Is all of this technology and expense worth the loss of personal privacy? In the past, individuals were able to opt out of being monitored by living without cell phones, PDAs, accessing the Internet and purchasing the latest technological gizmos for their cars. Now they cannot. What are we going to do to avoid being monitored and controlled? Should we remove our eyes or stay home all day?

Foucault, Michel. 1977. *Discipline and Punish* (trans. A. Sheridan). New York: Pantheon Books.

Minority Report. 2002. Film. Directed by Steven Spielberg. USA: DreamWorks.

O'Harrow, Richard. 2005. *No Place to Hide*. New York: Free Press.

Orwell, George. 1977. *1984*. New York: Penguin.

Pasqua, Charles. 24 February 2000. "U.S. accused of eavesdropping / European report claims surveillance used for trade gains." In *Houston Chronicle*. Houston: The Hearst Co., pp. 18.

Port, Otis. and Resch, Inka. 31 May 1999. "They're listening to your calls." In *Business Week*. New York: McGraw-Hill, pp. 10-11.

"The End of Privacy." 1999. In *World Press Review* 46(5). New York: Stanley Foundation, pp. 35.

The U.S. Department of Homeland Security. 2004. http://www.dhs.gov. Accessed 18 October 2004.

The U.S. Department of State. 2008. http://travel.state.gov/passport/eppt/eppt_2498.html. Accessed 27 April 2008.