# Borders, surveillance, and control in the digital age

David R. Burns
Southern Illinois University Carbondale
Department of Radio-Television
1100 Lincoln Drive, MC: 6609
Carbondale, IL 62901-6609 USA
*drburns@siu.edu*

**Borders, surveillance, and control in the digital age explores the way in which public and private institutions leverage electronic surveillance technologies to monitor and control individuals' personal communications, information, and movement across physical and virtual borders. Public and private institutions' transition from an emphasis on using physical border controls to an emphasis on using virtual border controls reflects a paradigm shift from a disciplinary society to a controlled society. Whereas in the past, visas and passports offered only a limited amount of individuals' personal data at physical borders, electronic surveillance technologies allow nations and institutions to instantaneously collect, monitor and control a vast amount of personal data from decentralized virtual access points. These decentralized virtual access points add a digital dimension to Foucauldian panopticism and expand the ways in which nations and institutions can continually monitor and control individuals within, across and outside their borders. In this essay, I investigate three major apparatuses of physical and virtual border control: global communications monitoring, ubiquitous tracking technologies, and biometrics and electronic databases.**

*borders, biometrics, control, computing, data, digital, information, institution, international, monitoring, networks, panopticon, surveillance, tracking, ubiquitous, us-visit, virtual, visit-us, government, public, private*

## 1. INTRODUCTION

Electronic surveillance technologies are being leveraged to monitor and control people's communications and movements within, across and outside borders. In this essay, I categorize three major apparatuses of control used to design and monitor virtual borders: global communications monitoring, ubiquitous tracking technologies, and biometrics and electronic databases. The developments in and the use of these surveillance technologies provide a comprehensive system for monitoring and controlling individuals and their data across physical and virtual borders.

## 2. TIER I: GLOBAL COMMUNICATIONS MONITORING

Nations have been active in monitoring global communications for many decades. However, the world's citizenry has never been exposed to a more comprehensive global communications monitoring system than Echelon. Echelon is a global network of listening stations and satellites that monitors all forms of electronic communications that cross international borders; land and cellular phone calls, faxes, e-mail and radio signals are examined, recorded and cross-referenced as they move through and across borders.

Echelon originated from a clandestine Anglo-alliance agreement 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 accessing and monitoring worldwide communications from Europe, Africa, Asia, Australia, North America and South America. As part of the program, each of the Echelon member countries' intelligence agencies was responsible for monitoring and gathering global communications in its area of the world (Port and Resch, 1999).

In 1999, the Echelon program gained critical media attention in a BusinessWeek article that described

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 sorting for keywords. The article explained how supercomputers could pick up strings of keywords from communications and forward them to human analysts for review (Port and Resch, 1999). Non-Anglo countries have voiced concerns about Anglo-alliance countries using the Echelon program's privileged surveillance information for purposes other than security aims. In 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 for international commercial contracts (Pasqua, 2000).

Until 9/11, Echelon and the US National Security Agency's surveillance efforts were primarily focused on monitoring communications among parties outside the Anglo-alliance. After 9/11, this model changed when the Bush administration instructed telecommunications companies to share US citizens' phone records with the National Security Agency. In July 2008, the US Congress approved legislation that granted immunity to telecommunications businesses that shared private customer information with the government. These businesses were released from following legal protocols when they supplied the National Security Agency with phone records and personal information on US citizens.

After 9/11, the US government's data mining effort was expanded beyond phone records to include personal data on millions of US citizens. As Isikoff (2008) reported, "the NSA's computers have access to—and crunch—wire transfers, bank transactions and reams of other personal financial data collected by the Treasury Department". This type of personal information is easy to acquire from data mining companies like Axicom, travel agencies, and government offices like tax and licensing authorities.

This monitoring of information indicates a paradigm shift from the US government's physical control and physical monitoring of individuals to its virtual control and virtual monitoring of individuals. In the classic Foucauldian model of control and discipline, if a disciplinary institution 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). When the US and its allies adopted the Echelon program and the US granted increased immunity to businesses that share private customer information with the government, there was a paradigm shift from the physical control and monitoring of individuals via search warrants for physical sites to the virtual control and monitoring of individuals via surveillance networks. With the use of listening posts, satellites, electronic networks and supercomputers to monitor phone calls and email, the old model of local physical controls over individuals' communications within and outside of physical borders broke down and was replaced by a electronic decentralized apparatus of control that transcended physical borders.

Government-sponsored monitoring of global communications also relies on visual data such as video surveillance. The strongest example of ubiquitous video surveillance exists in the United Kingdom. According to the London-based Information Commissioners Office, Britain has over 4.2 million surveillance cameras in operation, or 20% of the world's closed-circuit cameras. The Information Commissioners Office found that "there is a camera for every 14 people and an average Londoner is captured on camera 300 times a day" (Stinson, 2008). Called the "most monitored society in the world," London is almost impossible to pass through without being observed on a closed-circuit camera (Stinson, 2008). Although the government's stated intention for these cameras is the reduction of crime and terrorism, these cameras have been used to monitor minor offenses. For example, after cameras recorded a dog squatting in Bristol, law enforcement used the images to fine the dog's owner for "dog fouling" (Stinson, 2008). In a similarly minor offense, police used cameras to verify an English family's home address after the family had requested a special public service (Stinson, 2008). While these two scenarios sound benign, they conjure images reminiscent of Orwell's 1984 and create potential abuses of personal privacy.

The ubiquity of surveillance cameras in public spaces helps people become desensitized to electronic monitoring in public spaces. This allows for the use of surveillance devices to grow exponentially with little fanfare or resistance from the public. Lyon (2006) speaks to the cultural acceptance of surveillance technologies when he discusses the "cultural trends that render surveillance progressively more commonplace, unexceptional, and even desirable." (Lyon, 2006). As the use of surveillance devices in the public space grows, courts are revisiting the rules on using surveillance against citizens. England's Ken Jones, President of the Association of Chief Police Officers, told police chiefs that "abusing surveillance powers causes 'widespread unease' in the public and needs to be stopped" (Stinson, 2008). Legal systems struggle with achieving a

balance between providing security in public spaces and protecting individuals' personal privacy.

## 3. TIER II: UBIQUITOUS TRACKING TECHNOLOGIES

Ubiquitous tracking technologies including GPS chipsets, portable satellite receivers, and mobile data connections are commonly installed in a dizzying array of personal devices and vehicles. Many governments, including those in the United States and Britain, require manufacturers to install locative technologies like GPS chipsets in consumer mobile phones. These governments' justification for this requirement is to allow rescue and police teams to monitor and track down an individual's precise location in an emergency (CNET News, 2010). This type of government mandated policy is a major shift away from controlling and monitoring an individual's static, physical address to controlling and monitoring an individual's mobile dynamic address. As an example, in the past, state agencies waited for warrants to monitor individuals in fixed locations like their homes. The individuals were also handed a warrant by these agencies before law enforcement officials entered individuals' private spaces. Now, individuals' movement outside the border of their home can be dynamically monitored through their cell-phones without the individuals' knowledge and often without a court-issued warrant (Stanley Foundation, 1999).

The ability of government institutions to monitor and track individuals using their mobile phones without a warrant opens a new chapter in prospective electronic border surveillance. The Fourth Amendment was designed to guard individuals against the unreasonable search and monitoring of an individual by government agencies without probable cause or a court ordered search warrant. In 2010, US police and security agencies requested an order allowing for telecommunications companies to share the minute-by-minute location of mobile devices with local and federal law enforcement. In this order, the Obama administration was quoted as saying monitoring without warrants is permitted because Americans enjoy "no reasonable expectation of privacy" in their mobile phones' location (McCullagh, 2010). US Department of Justice lawyers argued that "a customer's Fourth Amendment rights are not violated when the phone company reveals to the government its own records" showing the location where an individual's mobile device is used (McCullagh, 2010). The US government's recent interest in real-time locative data, known as prospective data, signals a shift in government interest away from retrospective data and toward prospective data. Retrospective data is older, contains less detailed information, and is kept by telecommunications companies for billing purposes. Traditionally, government agencies have been required to obtain a warrant to eavesdrop on an individual's personal communications or to obtain their personal communications records from telecommunications companies. This retrospective interest has changed to prospective interest. With the order, US agencies have the potential to intercept individuals' communications in real-time and gather their personal communications records without requesting a warrant.

Non-governmental institutions also no longer view individuals as fixed targets within a postal code's physical geographic border. The continued miniaturization and pervasive use of GPS chipsets and mobile communications tracking technologies allow non-governmental institutions, like retailers, to identify people dynamically using their mobile phones. For example, it is now possible for retailers identify, target, and send electronic promotions to 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 where a number of storefronts directly market to the main character, Officer Anderton, as his physical location shifts in real time (Spielberg, 2002). Officer Anderton is tracked, targeted and solicited by biometric scanners that read his eyes. This Hollywood style of biometric tracking is here: the French company, Quividi, developed software for advertisers to calculate a person's gender and age using hidden cameras inside advertising displays that read people's faces (WNYC, 2009).

A similar type of tracking system could be applied to an individual driving his car within and across physical and virtual borders. More and more new vehicles are being bundled with pre-installed GPS or satellite technologies such as OnStar and satellite radio that enable drivers to be monitored. One of the more popular illustrations of this was the Hot Date television commercial in which the internal OnStar system in Batman's car monitors his location at all times (ONSTAR, 2001). Mobiltrak, a marketing company, has created a real-world example of this type of tracking system. Mobiltrak developed a "consumer monitoring system" technology housed in highway billboards that gathers information about individuals by intercepting radio broadcasts leaked from their vehicles (Salladay, 2002). It is easy to imagine a networked array of billboards that receive and transmit information about individuals driving by these billboards on stretches of interconnected highways.

In addition to monitoring and controlling mobile phones and vehicles, governments are beginning to monitor the vast amounts of personal electronic

data stored on individuals' portable hard drives when individuals travel across borders. As consumers continue transferring their office files to mobile devices, searches of laptops, cell phones, and PDAs may reveal sensitive information that was previously unavailable at border searches. While the Fourth Amendment of the US constitution provides protection against unreasonable search and seizure without probable cause, the legal ground is shifting toward searching individuals' portable offices, laptop computers and mobile devices at borders without probable cause or a search warrant. In April 2008, the Ninth Circuit court overruled a decision that prohibited airport officials from searching the data on a laptop's hard drive without probable cause. According to Worthen (2008), "the court concluded that a computer is a vessel used to transport something and that other such vessels – a sealed container, for example –are subject to search without cause at borders". The courts are expanding searches at border crossings to include personal data on mobile electronics devices. As mobile devices like the Apple i-phone are used as mobile offices, unsuspecting travelers may inadvertently offer up sensitive medical, financial and business documents in airport searches conducted without probable cause.

The security benefits that searches at borders provide are compelling in the post 9/11 era. However, while searching electronics hardware for explosive devices may be necessary to provide travelers with better security, searching travelers' personal virtual files on their mobile devices without probable cause creates the potential of infringing on the privacy of thousands of law-abiding travelers. According to Susan Gurley, a spokesperson for the Association of Corporate Travel Executives, "7% of business travelers have been subjected to the seizure of a portable device" (Gannett News Service, 2008). In the past, US search warrant requests were granted after being reviewed by a court. Now, the US Customs and Border Protection and the Department of Homeland Security can immediately confiscate and search travelers' mobile offices, such as PDAs and cell phones at border crossings without waiting for judicial review (Gannett News Service, 2008).

The growth in the forms of ubiquitous tracking technologies described above leave individuals with very few choices for circumventing the gaze of government and private surveillance, monitoring and tracking. Individuals can opt out of owning mobile phones, PDAs, or installing the latest technological gizmos in their vehicles. It is the technological components in these individuals' consumer items that are being tracked across physical and virtual borders. The individual in his organic form is less relevant. He or she is just the transportation mechanism for an electronic, ubiquitous transmission, reception, and tracking system. In the future, as biometrics replaces these electronic devices, it will be more challenging to opt out of being tracked across borders.

## 4. TIER III: BIOMETRICS AND ELECTRONIC DATABASES

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. Biometrics are defined by the US Department of Homeland Security (2005) as automated methods of recognizing a person based on "a physiological or behavioral characteristic that are unique to an individual." Physical biometrics include fingerprints, hand geometry, facial patterns, and iris and retinal scans. Behavioral biometrics include voice patterns, written signatures, and keyboard typing techniques" (US Department of Homeland Security, 2005). I believe that this emerging area of research and development will have a profound impact on the future of personal information and movement; it is where the organic and the virtual will collide in a seamless manner.

One of the largest projects designed to monitor and control individuals' movements within and across borders using biometric identifiers is the US-VISIT program. The US-VISIT program was designed to provide biometric identification services to federal, state and local government agencies to identify individuals' identities before, during, and after crossing US borders (US Department of Homeland Security, 2010). In January 2004, US-VISIT entry procedures were operational at 115 airports and 14 seaports (US Department of Homeland Security, 2004a). By 2006, the number of US-VISIT biometric entry scanning facilities mushroomed to include nearly all land border points of entry to the United States (Stana, 2007). Although not required yet, in the near future, all US airports, seaports, and land borders will require international visitors to submit to biometric scanning before exiting the United States (US Department of Homeland Security, 2008).

The US-VISIT program is not restricted to US soil. According to the US Department of Homeland Security (2010), 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" (US Department of Homeland Security, 2004c). The US Department of Homeland Security (2004b) 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 US Department of Homeland Security (2004b), 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. Before a visa is issued, this biometric data is checked against suspected terrorist watch lists. When an international 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 (US Department of Homeland Security, 2004).

Since August 2007, US citizens applying for or renewing their passports have been issued e-passports containing chips that store personal data. Older US passports without these chips will be valid until their expiry period (US Department of State, 2008). In my opinion, these policy changes in the way personal information is electronically checked at borders in real-time using biometrics indicate a clear a shift in US internal policy away from a disciplined society to a controlled society. In a disciplined society, US citizens would make choices to follow laws regarding presenting paper documentation to enter and exit borders. However, in my opinion, the US Department of Homeland Security seems to want to shift away from a disciplined society towards a controlled society. In a controlled society, US citizens who comply with biometric sampling when crossing physical borders have their biometric data automatically sent across electronically controlled systems of computer networks. Electronic data is automatically collected through real-time scanning of individuals' fingers and e-passport chips.

In this controlled society model with passports containing chips that store personal data and biometric scanning at borders, individuals do not have the ability to restrict the personal information that is entered in interconnected national and institutional databases. Whereas in the past, paper-based visas and passports offered a limited amount of an individuals' personal information at physical borders, the electronic, real-time gathering of personal information using computer networks allows institutions to instantaneously collect, monitor, and control a far greater amount of personal data from decentralized virtual access points. These electronic databases and networks add a digital dimension to Foucauldian panopticism and expand the ways in which nations continually monitor and control visitors' crossing their borders.

The role of educational institutions in collecting and sharing student information with external institutions is another area of critical importance. For example, the US Department of Homeland Security, US Department of Education and US Department of Defense have each argued for the creation of comprehensive student databases to monitor and track US and international students. This type of monitoring and control over minors and students requires thoughtful examination of the role of education institutions in providing layers of surveillance and control over students within and across deterritorialized educational borders.

The US Department of Homeland Security administers the Student and Exchange Visitor Information System (SEVIS) in connection with the US-VISIT program. SEVIS was designed to track and monitor international students before they arrive in and during their stay in the US. SEVIS includes data on close to a million foreign students, exchange visitors, and their dependents that is collected before they enter, when they enter, and during their stay in the US. This information includes "biographical information of the student or exchange visitor and their dependents (name, place and date of birth, spouse and children's data); academic information (status, date of study commencement, degree program, field of study, institutional disciplinary action); employment information (employer name and address, employment beginning and end dates); school information (campus address, type of education or degrees offered, session dates), and exchange visitor program information" (Electronic Privacy Information Center, 2005). This information combined with the personal information collected for obtaining a visa through the US-VISIT program builds a well-defined profile of students and visitors in the US. However, this type of program is not restricted to international students.

The US Department of Education has expressed its desire to monitor and track US students. In 2005, the Department of Education released a feasibility report for a national Student Unit Record System to track US students using individually identifiable information such as "name, Social Security Number, date of birth, address, race/ethnicity, gender, and field of study that are attached to an individual student's record" (Cunningham, A., Milam, J., & Stratham C., 2005). The system would also include academic performance, receipt of financial aid from federal, state, and institutional sources and track students as they move to different institutions (Cunningham, A., Milam, J., & Stratham, C., 2005). The US Department of Education is continuing to develop plans for this student surveillance system that would be accessible to not only to the US Department of Education, but also to the US Attorney General's office and the US Justice Department for national

security purposes (Electronic Privacy Information Center, 2005).

In 2003, the US Department of Defense also began compiling a large-scale student database of personal information for recruiting purposes. The US Department of Defense has proposed that it plans to continue gathering personal information on American students including minors as young as 16 years old. According to the Electronic Privacy Information Center, the database will be "managed by a private direct marketing firm and will include such information as grade point average, ethnicity, and social security number" of each student (Electronic Privacy Information Center, 2005). The US government entering into a large scale marketing agreement and capitalizing on students' personal information is a new development in the way the government agencies are accessing and controlling their citizens', including minors', personal information for non-security related projects. Bogard (2006) comments that control over "access to data on you, but not by you, is the goal of police (corporate, state) control of surveillance networks". Government's use of personal student information for marketing purposes is a new development in the way governments are leveraging the formerly private information they collect on citizens of all ages.

These three programs, SEVIS, Student Unit Record System, and the DOD database; combined with the US-VISIT program illustrate the creation of a powerful Orwellian surveillance system to track international and US students across and within US borders. The US Department of Homeland Security has already granted the FBI access to SEVIS and US-VISIT (Field, 2004). This new area of collaboration between academic institutions and government agencies to track and monitor students is a critical area to watch for potential abuses of personal privacy.

A critical issue to consider is who or what governmental and non-governmental institutions have access to all of the personal information being collected and for what purposes? The US Department of Homeland Security reports that the US-VISIT program "provides biometric identification and analysis services to federal, state and local agencies" (US Department of Homeland Security, 2008). In the past, the US Department of Homeland Security required that airlines and cruise companies report personal passengers' information to them. If this information is combined with individuals' credit card information, a more complete profile of each individual 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 data has been shared with the US government since 9/11 (O' Harrow, 2005). When this data is combined with information from SEVIS and the Department of Defense databases, government and non-government institutions have the potential to create a more complete system that can be used to profile, index, track and monitor individuals.

## 5. CONCLUSION

The tiers of surveillance technology used to monitor, track, and control individuals' movements within, across and outside borders described in this paper indicate a shift from public and private institutions' physical control and physical monitoring of individuals to their electronic control and electronic monitoring of individuals. This type of electronic, panopticonal surveillance and control ranges from government satellites, which monitor individuals' communications, to portable electronic devices, which provide information about individuals' physical locations, to virtual border controls, which allow institutional border control programs to automatically read individuals' biometric data. Private and public institutions' use of these new surveillance technologies has allowed older models of localized, physical controls over individuals within, across and outside of physical borders to be replaced with an electronic, decentralized apparatus of control that transcends physical borders. Public and private institutions' use of this electronic, decentralized apparatus of control to track individuals' vehicles, portable electronic devices and biometric data presents potential concerns about individuals' personal privacy.

Public and private institutions are moving toward a ubiquitous, seamless model of surveillance and control that extends beyond tracking and monitoring individuals' physical movements across international borders to tracking and monitoring individuals' physical and virtual movements across localized micro-borders such as streets, stores, and homes. This new model relies not only on deterritorialization and biometrics but also on individuals' electronic identities. In the past, individuals were able to opt out of being monitored and controlled by living without mobile phones, the latest technological gizmos for their vehicles, and traveling across distant physical borders. Now individuals can no longer avoid the gaze of surveillance and prevent the collection of their personal information as they move across localized physical and virtual borders.

## 6. REFERENCES

Bogard, W. (2006) Surveillance assemblages and lines of flight. In D. Lyon (ed), *Theorizing surveillance; The panopticon and beyond*. Willan, UK.
Cunningham, A., Milam, J., & Stratham C . (2005, March) Feasibility of a student unit record system within the integrated postsecondary education data system. U.S. Department of Education, Washington D.C.
Electronic Privacy Information Center. (2005) SEVIS database tracks every move of foreign students, visitors. http://epic.org/privacy/surveillance/spotlight/0905/default.html (10 September 2005)
Electronic Privacy Information Center. (2005) US-VISIT rolls out the unwelcome mat. http://epic.org/privacy/surveillance/spotlight/0705/ (15 July 2005)
Field, K. (2004). FBI gets access to student databases. The Chronicle of Higher Education http://chronicle.com/article/FBI-Gets-Access-to-Student-/36101. (22 August 2010).
Foucault, M. (1977) Discipline and punish (trans. A. Sheridan). Pantheon Books, NY.
Gannett News Service. (2008) Electronics subject to search at border. USA Today. http://www.usatoday.com/tech/news/techpolicy/2008-07-06-laptopsearch_N.htm. (7 July 2008).
Isikoff, M. (2008) Uncle sam is still watching you. *Newsweek*. pp. 6.
Lyon, D. (2006) 9/11, synopticon, and scopophilia: Watching and being watched. In K.D Haggerty & R.V. Ericson (eds), *The new politics of surveillance and visibility* pp. 35-54. U of Toronto Press, Toronto.
McCullagh, D. (2010) Feds push for tracking cell phones. CNET News. http://news.cnet.com/8301-13578_3-10451518-38.html (11 February 2010).
Mintz, J. (12 July 2005) Clearing customs with an eye scan. *The Wall Street Journal*, pp. D4.
O'Harrow, R. (2005) No place to hide. Free Press, NY.
ONSTAR. (2001) Hot Date, Television advertisement, ABC. Screened 25 March 2001. Campbell-Ewald Advertising, USA.
Orwell, G. (1977) *1984*. Penguin, NY.
Pasqua, C. (24 February 2000) US accused of eavesdropping / European report claims surveillance used for trade gains. *Houston Chronicle*, pp. 18.
Port, O. & Resch, I. (31 May 1999) They're listening to your calls. *BusinessWeek*. pp. 10-11.
Salladay, R. (2002) High-tech billboards tune in to drivers' tastes. San Francisco Chronicle. http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2002/12/22/MN242772.DTL (18 August 2010).
Spielberg, S. (2002) Minority Report (Film). DreamWorks, USA.
Stanley Foundation (1999) The End of Privacy. *World Press Review*, 46(5). pp. 35.
Stana, R. (20 March 2007) Homeland Security: US-VISIT Program Faces Operational, Technological, and Management Challenges. US Government Accountability Office, Washington D.C.
Stinson, J. (7 July 2008) Anti-terror cameras catch banal offenses. *USA Today*. pp. 7A.
Taylor, J. (2000) Project Echelon. *Reason*, 31: 9, pp. 12.
US Department of Homeland Security. (7 January 2005) US-VISIT increment 2C, proof of concept – Concept of Operations Phase 1. US-VISIT Program Office.
US Department of Homeland Security (2004a) http://www.dhs.gov/xnews/releases/press_release_0539.shtm (19 August 2010).
US Department of Homeland Security (2004b) http://www.dhs.gov/xnews/releases/press_release_0476.shtm (22 August 2010).
US Department of Homeland Security (2004c) http://www.dhs.gov/xnews/releases/press_release_0573.shtm (22 August 2010).
US Department of Homeland Security (2008) http://www.dhs.gov/xlibrary/assets/usvisit/usvisit_edu_air-sea_biometric_Exit_Update.pdf (20 August 2010).
US Department of Homeland Security (2010) http://www.dhs.gov/files/programs/usv.shtm. (22 August 2010).
US Department of State (2008) http://travel.state.gov/passport/eppt/eppt_2498.html (27 April 2008).
US Department of State (2010) http://travel.state.gov/law/legal/testimony/testimony_789.html#. (18 August 2010).
WNYC (6 February 2009). An eye for an eye (broadcast). On The Media, NY.
Worthen, B. (2008) Court: Your laptop is luggage, may incriminate you. The Wall Street Journal. http://blogs.wsj.com/biztech/2008/04/23/court-your-laptop-is-luggage-may-incriminate-you/. (23 April 2008).