Surveillance & Society
Special Issue on 'Surveillance and Criminal Justice' Part 1, 4(3): 208-228
http://www.surveillance-and-society.org

Escalating U.S. Police Surveillance after 9/11: an Examination of Causes and Effects*

William Bloss[1]

Abstract

In recent years U.S. police have been given greater surveillance powers in response to perceived threats from crime, drugs, and terrorism. Several legal and criminal events have facilitated a reevaluation of the balance between police surveillance authority and civil privacy protection. In the post-9/11 era, changes in federal law, court interpretation of privacy safeguards, and technological advances have expanded the circumstances and methods by which the police may engage in surveillance of civil activities. This paper examines the factors contributing to the escalation in police surveillance and its effects on privacy rights and civil life. The analysis suggests that increasing police surveillance has diminished individual privacy protections and impacted aspects of civil life.

Introduction

Views of surveillance and privacy have changed dramatically in recent years. Some commentators assert that the U.S. has experienced a progressive shift in the balance between police surveillance authority and individual privacy rights (Chang, 2003; Bloss, 2005). Others cite the terrorist attacks on September 11, 2001 (9/11 hereafter) as a watershed event that provided the catalyst for the widening of police surveillance and search authority (Posner, 2003; Romero, 2003). The record is replete with examples of U.S. official responses to perceived public safety threats that have precipitated an increase in police surveillance activity (Brown, 2003). Events such as the detention of Japanese descendents during World War II, McCarthy anti-communist investigations, anti-crime campaigns, anti-drug wars, and current counter-

* An earlier version of this paper was presented at the Crime, Justice, and Surveillance conference at the University of Sheffield. This paper benefited from the comments of anonymous reviewers and the author appreciates their valuable suggestions. Also, the author gratefully acknowledges the support provided by The Citadel Foundation in the completion of this study. The views expressed herein are those solely of the author.

[1] Department of Political Science and Criminal Justice, The Citadel, South Carolina, USA.
mailto:blossw@citadel.edu

 ISSN: 1477-7487

terrorism policies provide evidence that U.S. public safety strategies commonly involve a prominent police surveillance and search role (Cole, 2003; Abrams, 2005). Faced with modern transnational crime and terrorism, operating in a technologically fluid global environment, the extant official strategy obligates the police to ensure greater public safety under increasingly unpredictable circumstances (Posner, 2003; Stohl, 2003; Kugler and Frost, 2001). In what Cole (2003:13) refers to as "preventive law enforcement," the legal and operational response has been to use greater surveillance to reduce threats and prosecute transnational offenders. Since the police often lack the manpower and technical expertise to keep pace with global terrorists and criminals, they have widened their surveillance capability by collaborating with private commercial enterprises to obtain personal data or to eavesdrop on the public (O'Harrow, 2005; Bridis and Solomon, 2006).

The central position of this paper is that U.S. lawmakers and courts have reacted to perceived global terrorism and crime threats by modifying established civil privacy protections, under the aegis of "preventive law enforcement," thereby giving the police broader surveillance powers (Cole, 2003). As a result, the police have transformed their operational approaches and surveillance practices to focus more on information and intelligence gathering (Peterson, 2005; Carter, 2004). This has produced a new privacy paradigm, as the balance between police surveillance authority and civil privacy protection shifts. This paper explains the factors that have caused or contributed to this transition and its effect on civil privacy and civil life in U.S. society.

The paper first examines the legal and political causes for the change in the "competing interests" balance between official surveillance and individual privacy protection (*O'Connor v. Ortega*, 1987). Second, it discusses the operational and programmatic emphasis U.S. police are now placing on surveillance methods and data. Third, it explores the effects of these changes on civil privacy rights and civil life. These include the disruption of public life, "net widening" of police surveillance activities, and diminution of personal privacy rights (Laqueur, 1999).

Conceptualizing Surveillance

Conceptually, "surveillance" can be viewed from different perspectives. In the context of this paper, surveillance is explained as the police activity of gathering information on individuals. First, it includes human and technological gazing where officials watch the physical movements and activities of persons. Second, surveillance involves the acquisition of personal data. This includes the collection of biographical, biometric, or transactional data on individuals harvested from personal communications, electronic transactions, identifiers, records, or other documents. In the former, observations can be used for identification or may act to advance an investigation as a component of a larger body of evidence, as in the case of CCTV data. The latter involves voice or documentary information that can be used in criminal investigations or prosecutions. Hence, the meaning given to police surveillance here is the collective action of official gathering of information on persons for the stated purpose of preventing crime and terrorism or prosecuting offenders. As the police gather more personal information through surveillance, search, and seizure, a greater number of persons come within their official purview vis-à-vis suspicion profiles, threat assessments, or specific investigations (Romero, 2003).

Under U.S. law, police and other government officials are subject to specific guidelines which govern their authority to intrude into the activities of citizens for the purpose of criminal investigation, gathering of evidence, or criminal prosecution. Official intrusion consists of three activities— surveillance, searching, or seizing (del Carmen, 2004). As a police practice, surveillance is the collecting of investigative observations or data; searching for evidence is the probing into personal activities or belongings to discover incriminating evidence; seizing of evidence is the taking of items to be used in criminal investigations or prosecutions. Originally, police surveillance and search practices were strictly for detecting evidence for criminal prosecutions. However as this paper argues, increasingly police surveillance is also being used for the *preventive* purpose of gathering information on persons perceived to be crime or terrorist threats (Cole, 2003). Thus, the result has been to expand both the reach and authority of the U.S. police to engage in these activities.

Expanding Police Surveillance

Americans have long been concerned about government surveillance (Albanese, 1984). Because of its democratic ideals and commitment to an equitable balance between government power and civil liberty, U.S. citizens are accustomed to wrestling with this political issue. As noted, perceived threats from crime, drugs, and terrorism have been used as a justification to expand government social controls. Whitaker (2003: 52) claims that "the historical cycle in which violent threats generate the expansion of arbitrary and intrusive powers of government is being repeated. Once again, the constitutional protection of rights is being dismissed, sometimes from the highest offices in the land, as an inconvenient impediment to safety."

U.S. police have been given greater legal and procedural latitudes to conduct a wider range of surveillance activities involving criminal and terrorist counter-measures and investigations (Brown, 2003). Several legal, political, and technological factors have contributed to the increase in the use of police surveillance methods. Some of these contributors stem from recent global events. Clearly, factors such as globalization effects, modern terrorism and transnational crime threats, and advances in electronic technology have joined in changing the perspective of public safety, public threat assessment, and crime control (Kugler and Frost, 2001; Berdal and Serrano, 2002; Kegley, Jr., 2003; Friedman, 2005). Domestically, antecedent socio-political events and legal changes in police surveillance and search powers have created an environment that is conducive to the escalation of official surveillance. All told, a myriad of factors have led to a transformation in the relationship between privacy laws, police surveillance practices, and public privacy expectations in the United States (O'Harrow, 2005; EPIC, 2006).

Over the past two decades, courts and statutes have dismantled several traditional privacy and search safeguards to ostensibly allow the police to be more effective in combating crime, drugs, and terrorism (Bloss, 1996). Through a series of changes in legal doctrine and enactment of new legislation, dramatically accelerated after the 9/11 incidents, the U.S. police have acquired unprecedented surveillance, search, and seizure authority. Earlier campaigns such as the "war on drugs" provided the initial impetus for these changes (Bandow, 1991). However, modern global terrorism has caused a reassessment of public risk that has led the police to shift their practices to respond to these perceived threats. Part of the operational formulae is widening the scope of

surveillance and information gathering in an effort to avert future terrorist attacks (O'Harrow, 2005).

Given the rise in transnational crime and terrorism in recent years, some have suggested that a "global perspective" is the most relevant approach to contemporary analyses of these phenomena (Williams and Savona, 1996; Williams, 1999; Andreas, 2002; Shelley, 2005; see generally Bloss, 2006). Though this influence is not overlooked, this paper purposefully focuses on legal and political changes in U.S. citizen privacy rights in relation to the increased surveillance powers given to its police. In doing so, it is necessary to frame the discussion in the context of legal and socio-political privacy traditions in American society. In spite of this emphasis, other influences have also contributed to shaping the transformation in the U.S. Among those are the effects of globalization and technology. Both have affected modes of information, commerce, communication, identity and susceptibility to crime victimization, as well as the manner in which the police combat crime.

Factors Contributing to the Widening of Police Surveillance

Globalization of Crime and Terrorism

Globalization has changed many aspects of political, economic, and civil life worldwide (see Berdal and Serrano, 2002; Thachuk, 2001; Messner, 2002). Many of the same conditions that promote multinational alliances and improve trade among legitimate states also benefit transnational criminals and result in increased public safety threats (See Siegel, van de Bunt, and Zaitch, 2003; Reichel, 2005; Bloss, 2006).

As crime and criminals cross national borders, police face new challenges in promoting public safety, investigating crimes, and apprehending offenders (Grabosky and Smith, 1998; see Kegley, Jr., 2003). In many cases, crime scenes have changed from stationary locations to ephemeral digital sites (see Taylor et al., 2006). And criminal offenders have become increasingly adept in the use of technology to perpetrate transnational illegal acts (i.e., terrorism, drug trafficking, human trafficking, organized crime, etc.) (Grabosky and Smith, 1998). Perceived threats, posed by global terrorists and criminals, have provided the impetus for many of the legal changes that have contributed to the enhanced surveillance powers of the U.S. police in recent years (Whitaker, 2003; Bloss, 2005).

Advances in Technology

Changes in technology have contributed to the ability of the police to engage in electronic surveillance of citizens. Personal electronic communications (i.e., internet, voice-over-internet-protocol, cellular telephone, wireless transmission, etc.) are able to be intercepted with greater ease, and to some extent, with less physical intrusion. Therefore, part of the motivation for the police to increasingly adopt the use of electronic technology is to make them more effective at pursuing elusive criminals on a global scale. For some time, U.S. police have been asking for greater surveillance and search authority in an effort to keep pace with the technology use of

criminals.

Transforming the Privacy Framework

A change in U.S. civil privacy rights can best be understood in the context of the balance between government authority and civil liberties. American law entitles citizens to a fundamental "expectation of privacy" (*Katz v. United States*, 1967). This protection, however, has been affected by alterations in legal doctrine, new statutes, and counter-terrorism policies.

Citizen Expectation of Privacy Standard

Personal privacy rights are an integral part of the relationship between citizens and government in American culture. Though no constitutional mandate assures individual privacy, the courts have interpreted it as an inherent right possessed by all citizens (Ducat, 2004). Therefore, an expectation of personal privacy has become a cornerstone of American law and the doctrine has spawned a considerable body of statutory and case law (Reamey, 1992). As part of a larger civil liberty protection, American citizens have legal safeguards against police surveillance of their private activities.

Privacy doctrine prior to the 1960s was based upon the *Olmstead v. United States* (1928) standard. Though the *Olmstead* case dealt with electronic eavesdropping by the police, its "trespass" doctrine was noted for protecting "places" not people from government surveillance. In 1967, the United States Supreme Court crafted the "expectation of privacy" doctrine holding in *Katz v. United States* that citizens, who demonstrate a reasonable and subjective expectation of privacy, were protected from government intrusion. This landmark decision created a privacy standard that continues to be the prevailing legal doctrine in determining individual privacy protection from police surveillance (McAninch, 1991; Bloss, 1996).

Four decades after *Katz*, technological advances and global threats from terrorism and transnational crime have compelled lawmakers and courts to view citizen privacy safeguards in the context of the compelling need of the government to provide public safety. As seen with new statutes and reduced legal constraints on the police, allowed by the courts, the boundaries of individual privacy protection are now considered in a different context.

Balancing of Competing Interests Standard

Courts have devised a test to weigh the permissibility of police surveillance and search powers in relation to civil privacy. [2] A "balancing of competing interests" measure allows the courts to interpret constitutional principles and statutes to decide whether police surveillance and search

[2] U.S. courts interpret the legality of police surveillance and search practices in light of constitutional principles and/or court decisions. Police surveillance, search, and seizure are analyzed using constitutional privacy or search and seizure standards outlined in the Fourth Amendment to the U.S. Constitution, which prohibits unreasonable government searches and seizures.

methods violate citizen privacy. The balancing test can be used in various factual circumstances and has become the preferred court standard for making these determinations (Bloss, 2002). American courts also use this measure to determine whether the police should be allowed to use warrantless surveillance and search methods to promote public safety (*O'Connor v. Ortega*, 1987). [3] According to Chang (2003), the courts have tilted the balance more toward an increasing number of police intrusive measures to protect American society from the threat of global terrorism and crime. Thus, these interpretation methods have contributed to a reshaping of the traditional view of the *Katz* "expectation of privacy" standard.

Legal Changes in Police Surveillance and Search Authority

U.S. police are legally authorized to conduct surveillance and engage in search and seizure to gather prosecutorial evidence (del Carmen, 2004). Originally, the Fourth Amendment to the U.S. Constitution required the existence of a "probable cause" legal justification and court-issued warrant (U.S. Constitution IV Amendment). [4] These rigid standards have been relaxed through various legal exceptions. [5] However since the mid-1980s, courts have significantly changed legal guidelines which permit the police to conduct various types of administrative and warrantless searches (Bloss, 2005). Legal constraints on police surveillance and search activities have been dramatically reduced by new federal counter-terrorism laws (Whitehead and Aden, 2002). In the U.S., campaigns against public threats such as the "war on drugs" and "war on terror" have prompted the courts and lawmakers to make significant changes in the scope of civil liberties (Bandow, 1991; Whitaker, 2003). Particularly after 9/11, they have given rise to several federal laws that bestow greater surveillance powers on the police.

Pivotal Federal Surveillance Statutes

USA Patriot Act

Shortly after the September 11, 2001 terrorist attacks in the United States, Congress revised several federal laws allowing the police greater surveillance and search powers, as well as access to private information. The "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act," later known as the "USA Patriot Act of

---

[3] Police searches are conducted either with a court-issued warrant or without (warrantless). Since warrantless search decisions are non-judicial, and based on independent police discretion, they are often viewed by the courts as legally less desirable.

[4] Authorized police searches and seizures are based on three legal justifications. First, the requirement of "probable cause" explained as facts, information, or circumstances that would lead a reasonable police officer or jurist to believe that a crime has been committed. Second, the original Fourth Amendment required police to first obtain a court-ordered warrant to conduct any legal search or seizure. However under a third justification, the warrant requirement may be waived if the police search and seizure is conducted using court-established exceptions. These may allow for the use of warrantless searches where police are not required to obtain prior court authorization.

[5] U.S. courts have established a number of exceptions to the probable cause and warrant requirements, thereby, allowing the police to search without a warrant or use lesser legal standards such as reasonable suspicion; which is based simply on explained suspicion.

2001 (Patriot Act hereafter)," is considered the benchmark of these statutes (Whitehead and Aden, 2002). This legislation modified or revised fifteen federal laws, focusing primarily on counter-terrorism and foreign intelligence, and became the catalyst for statutory surveillance revisions. As indicated in Table 1, key provisions of the Patriot Act broadened police surveillance capability under several existing federal statutes.

Key Provision	Specific Effect
Amends several federal statutes	Foreign Intelligence Surveillance Act, Immigration and Naturalization Act, "Wiretap Act," Bank Secrecy Act and others.
Amends legal definitions	Domestic Terrorism, Foreign Intelligence Information, Warrant Certification.
Broadens police search powers	Surveillance, search, and intelligence gathering: Wiretap authority; Use of Pen Register and Trap/Trace Devices; Allows "sneak and peek" Search Warrants; Allows the use of Investigation "gag orders;" Monitoring Financial Transactions; and Required Disclosure of Educational Records.
Consolidates police power	President and Attorney General acquire additional intelligence gathering and investigative authority: Use of Investigation Certification Use of National Defense Letters
Expands domestic intelligence-gathering authority	Allows the Central Intelligence Agency to gather domestic intelligence on citizens

Table 1: **Key Surveillance Provisions in the USA Patriot Act**
(USA Patriot Act of 2001; Whitehead and Aden, 2002)

Redefining Crime and Investigative Definitions in the Patriot Act

One of the primary objectives of the Patriot Act was to provide the police with greater information access. Pursuant to that goal, it expanded the statutory definition of "domestic terrorism," "foreign intelligence information," and "terrorist organization" to provide the police with greater latitude in conducting investigations related to terrorism and foreign intelligence. Table 2 presents select amended crime and investigative definitions contained in the Patriot Act.

Terminology	Statutory Revision

Domestic Terrorism	"...involves acts dangerous to human life that is a violation of the criminal laws of the United States."
Foreign Intelligence Information	"...that relates to the U.S. ability to protect itself from attack, threats to national security or terrorism."
Alien Visitor Entry Denial	"[includes anyone who] represents a foreign terrorist organization [or is a member of a] political, social, or other similar group whose public endorsement of acts undermines U.S. efforts to eliminate terrorist organizations or supports or encourages others to support organizations."
Purpose of Special Surveillance Powers in the Foreign Intelligence Surveillance Act	Changes investigation purpose for allowing special search warrants and electronic surveillance from "only" purpose to "significant" purpose.

Table 2: **Amended Definitions in the USA Patriot Act**
(USA Patriot Act of 2001; Whitehead and Aden, 2002)

These revised definitions "widen the net" on potential illegal acts or actors thereby expanding the ability of the police to engage in surveillance or conduct investigations in a broader range of alleged criminal or foreign intelligence-related activities.

Enhanced Police Wiretap Authority

Patriot Act revisions also broaden police investigative capabilities by reducing some of the legal constraints of the Omnibus Crime Control and Safe Streets Act of 1968, Title III (Wiretap Act). It allows the police to request a wiretap search warrant, from the court, to engage in electronic surveillance if a need arises to investigate "any foreign intelligence information" for "terrorist," "chemical weapons," or "computer crime" investigations. The revised language of the Patriot Act lessens the more conventional *particularity* requirement whereby a specific alleged foreign intelligence activity must be demonstrated to obtain a wiretap warrant.[6]

Roving (Multi-Point) Wiretaps

Prompted by emerging technology, the Patriot Act instituted the use of "roving wiretap warrants" that allow the police to obtain a court-ordered warrant to engage in wiretap surveillance "against unspecified persons" across all domestic jurisdictions. This provision responds to the increasing use of mobile cellular and satellite telephones, voicemail messaging, voice over internet, and related technology which has subverted the restrictions placed on an earlier generation of hard-wire telephone technology. Further, the law provides for a "blank warrant," to be used in conjunction with the "roving wiretaps," that can be completed by federal police in any jurisdiction as needed. Hence, prior restrictions on police warrant requests, naming the known

[6] The traditional "particularity" standard requires the police to specifically state the identity of the known suspect, alleged crime, location, or evidence sought in a request for a court-ordered search warrant. In the case of foreign intelligence-based wiretaps, specifically naming the known suspect or illegal activity that is the focus of the investigation.

suspect, and specific stationary location for the wiretap warrant, have been supplanted by these revisions in the case of counter-terrorism or foreign intelligence investigations.

Pen Register and Trap Traces

Use of "pen register" and "trap and trace" devices, designed to record telephone number transactions from a fixed location, is an established surveillance method in wiretap-type investigations. Provisions of the Patriot Act expand their use to include the recording of computer "IP" addresses- a location identifier for a specific computer- and the warrant may permit the surveillance to extend anywhere in the United States. Again, these changes are designed to allow the police to have surveillance capability with emerging mobile and computer technology; where previous guidelines were intended to afford civil liberty safeguards based on more traditional crimes and existing technology.

Legal Standard to Obtain Wiretaps

Under the Patriot Act both probable cause, and its lesser legal standard reasonable suspicion, has been replaced by a "certification" requirement. [7] "Certification" only compels the police to state that the information sought in the wiretap warrant is "related to a law enforcement purpose." This reduced warrant standard places a lesser burden on the police to demonstrate specific facts to support their wiretap warrant request.

"Sneak and Peek" Search Warrants

Before the new provisions of the Patriot Act, police search warrants for a specific location had two legal requirements- announcement and notification. One exception to the announcement mandate was that federal courts could authorize "no-knock" search warrants where the police could demonstrate that alerting the suspect to their impending search would compromise officer safety or the preservation of evidence (del Carmen, 2004). "Sneak and peek" warrants authorize the police to conduct surreptitious searches or wiretaps without announcing their presence or notifying the person who is the target of the investigation at the time of the search. These unannounced searches allow delaying suspect notification if the police deem such information to have an "adverse effect" on the investigation (i.e., threat to safety, risk of flight, destruction of evidence or interference with the investigation). This change is a significant modification of the Fourth Amendment search warrant procedures previously established by the courts.

Imposition of Gag Orders

Another important reversal of the notification requirement is the provision for the use of "gag orders" where the court may prohibit business personnel from divulging to a patron that they are the target of a police investigation. When a federal police search warrant is used to wiretap computers or obtain patron records from a business (i.e., public library or bookstore) the merchant or employee can be prohibited from notifying the patron suspect. As with other applications under the Patriot Act, the police must affirm that these records or searches involve "foreign intelligence information" for the court to authorize the use of the "gag order."

---

[7] Certification is a reduced legal standard needed to obtain a court-ordered wiretap under the Patriot Act legislation. It is the least rigorous legal standard for police wiretaps and replaces the original probable cause and particularity requirements for warrant requests.

Monitoring and Reporting Financial Transactions
Several revisions of the U.S. bank reporting statutes are contained in the Patriot Act. Financial institutions are now required to report "potentially unlawful activity" on current or former bank customers or employees to the federal authorities. Financial institutions bear the burden of determining what may be potentially illegal activity. If related to a terrorism investigation, the law also allows the federal police to obtain financial information (i.e., credit reports, bank statements, financial reports, etc.) on bank patrons pursuant to a "financial analysis." Involving "foreign actors" who are the target of a "foreign intelligence" investigation, federal authorities are permitted to seize the bank accounts, assets, and property if ordered by the court. Courts may also impose "gag orders" upon financial institutions to prevent their employees from disclosing to the bank patron that they are the focus of an investigation.

Disclosure of Educational Records
Upon "certification" that the request involves a terrorism investigation, educational institutions are also required under the Patriot Act to disclose all educational records to the police, once directed by a court order.

Permanent Renewal of the USA Patriot Act
The USA Patriot Act has become the cornerstone of U.S. federal statutes that have expanded police surveillance authority after the 9/11 attacks. Sixteen of its original 2001 provisions were due to expire at the end of 2005. On March 9, 2006, each of the expiring provisions was renewed, and even though certain sections were embellished or had safeguards against government abuse added, it remained substantially unchanged. As an example of minor changes, Section 215 added "any tangible thing" (i.e., business records) as items that could be searched and seized by police pursuant to a foreign intelligence or counter-terrorism investigation. (See Electronic Privacy Information Center, 2006). Otherwise, the legislation retained its original contents and is being used to statutorily expand police surveillance and search authority in foreign intelligence and counter-terrorism investigations.

In spite if its influence in current U.S. law, the Patriot Act is not the only federal legislation that has enhanced police surveillance and search capabilities. Because of the increased public use of electronic communications, police wiretapping has become a much more common surveillance practice. Beginning in the mid-1980s, U.S. federal law established guidelines governing the interception of wire communications. The Electronic Communications Privacy Act (ECPA), enacted in 1986, has been substantially revised due to advances in technology and Patriot Act provisions. These revisions have been used to provide greater wiretap access in criminal or terrorism investigations (Kerr, 2004; Martin, 2006).

Electronic Communications Privacy Act

The U.S. Congress passed the Electronic Communications Privacy Act (ECPA) which is designed to provide statutory safeguards to protect citizens from government interception of electronic communications. The statute establishes legal guidelines for the government interception of voice and data over telephone, internet, and other forms of wire and wireless electronic communication. After passage of the Patriot Act, ECPA has been subject to revisions that allow the police to use court-issued search warrants to affix pen registers or trap and trace devices to telephone and internet service provider equipment to intercept electronic communications and data. To protect the investigation, the police can request a court-issued gag order be served on internet service providers (ISP) or communication service providers (CSP) to prevent them from divulging to patrons that they are the target of electronic interception. Under ECPA, police may also intercept electronic communications, without a warrant or court order, if they obtain the consent of one of the communication participants or an exigency exists. [8] The participant consent provision is available if allowed by state law in the jurisdiction where the police intercept the electronic information. Interception of electronic communication is authorized by ECPA in each of the following circumstances:

- With court authorized wiretap order;
- With participant consent;
- If the interception is necessary to protect the rights or property of the ISP/CSP;
- If the ISP/CSP inadvertently obtains information that pertains to a crime;
- If an emergency exists where there is an imminent risk of physical injury to a person; or
- If the system configuration renders the information readily accessible to the general public.

(Electronic Communication Privacy Act of 1986; del Carmen, 2004).

Under each of the circumstances both the internet service provider/communication service provider and the police are permitted to use pen register, trap and trace, or wiretap devices to obtain electronic communication voice and data for use in criminal investigations. Using subpoena or court order, the police can obtain basic subscriber or transactional information about patrons from the ISP/CSP. Additional user information can be acquired with a court order, which is based upon explanation of specific facts that support the request.

Increasing public use of electronic communication technology (i.e., cellular telephone, internet, etc.), complicates police surveillance (Bennett, 2005). Much of the technological advances in private electronic communication are protected by either federal statutes (i.e., Electronic Communications Privacy Act) or the courts. Particularly in the area of internet use, the police have had difficulty monitoring much of the information managed by private internet service or communication service providers because of incompatible wiretap surveillance equipment.

[8] Exigency is a legal term that describes an emergency circumstance that may compel the police to abandon standard search and seizure practices. Examples are imminent threats to personal safety, risk of destruction of evidence, or pursuit of an escaping suspect.

Communications Assistance for Law Enforcement Act (Digital Telephony Act)

At the request of the police, the U.S. Congress enacted the Communications Assistance for Law Enforcement Act (CALEA) in 1994 that requires internet service providers to give "easy access" to law enforcement for court-ordered surveillance, wiretapping, or data mining activities. CALEA requires ISP companies that use circuit-based telephone networks or packet-based data networks to calibrate their internet equipment so that it facilitates police wiretap access to the information transmitted through internet servers. The law broadens the access to cutting-edge technology such as DSL (telephone connected) and Broadband internet, cable, satellite, wireless, commercial "push-to-talk," and Voice Over Internet Protocol (VOIP) technology.

Regulated by the U.S. Federal Communication Commission, ISP/CSP providers in 2004 were directed to comply with CALEA by giving the police "easy access" to all equipment needed for court-ordered surveillance or wiretapping. CALEA also provides the police with the ability, through the ISP or CSP, to locate cellular telephone users, identify callers or determine telephone features (i.e., call forwarding, voice messaging, call waiting, etc.) used by the patron.

The U.S. police have responded to their greater surveillance authority by adapting operational practices and utilizing more technology to collect an unprecedented quantity of private information (see Chang, 2003; O'Harrow, 2005).

Police Surveillance and Operational Responses

Some scholars contend that, unlike past crime threats, modern terrorism poses unique risks to public safety (Laqueur, 1999; Kegley, Jr., 2003; Hoffman, 2004). Whitaker (2003: 53) describes the modern terrorist as "flexible, adaptable, diversified, transnational, de-centered, a network of networks." Since their motives, objectives, and tactics differ significantly from localized street crime, the police have altered their counter-terrorism approach to crime prevention and public safety (White, 2006; Bloss, 2006).

Central to this adaptation is their greater dependence on technology and surveillance to gather and disseminate information (Davis, 2004). Supported by new federal eavesdropping legislation, the police are working to be more effective at gathering a broad range of data on the public.

Emerging Police Surveillance Programs

Internet Surveillance

The U.S. Federal Bureau of Investigation developed an internet surveillance program known as "Carnivore" in the late 1990s (EPIC, 2005). When implemented, the program was designed to monitor internet traffic and gather user IP addresses, site visitation, and related user activity that were contained in a predetermined "packet" of information. The program used a surveillance protocol that relied on "filters" to restrict the collection to only authorized data within the designated packets of information. In 2002, the FBI canceled the program amid criticism that the filter and surveillance protocol allowed the interception of all information within its purview.

At that time, the FBI stated that it would refine the protocol and launch another internet surveillance program to replace Carnivore (Electronic Privacy Information Center, 2005). However, O'Harrow (2005) reports that law enforcement agencies have instead decided to conduct surveillance and collect citizen data through partnerships with commercial internet service providers, telephone companies, and data collection agencies. Rather than reinstate the tracking program, the FBI has opted to use commercially available software in addition to using private sector sources (Paulsen, 2005).

Foreign Visitor Surveillance

Since the terrorist attacks of 9/11, American police have devoted much more attention to foreign visitors entering the United States. Border security has been added to the terrorism national security threat assessment and the U.S. is militarizing its southern border with Mexico in an effort to disrupt the flow of human trafficking and contraband (Baker, 2006). As part of a larger initiative to monitor foreigners, the Department of Homeland Security and Transportation Security Administration have devised several programs to document and regulate visitors. Foreign visitor screening programs have gone through numerous changes since 2001. Originally, the Computer Assisted Passenger Prescreening Program (CAPPS) was developed to collect airline passenger data and to conduct background checks that were compared with secret "watchlists" maintained by the federal Terrorist Screening Center. The CAPPS I, and later CAPPS II program, gave way to the "Secure Flight" program. This program is designed to assess a passenger's terrorist threat risk using a computer algorithm. Airline passengers identified as a risk by "Secure Flight" are placed on a "no-fly" list and prevented from entering the United States.

One of the most recent versions, among the foreign visitor screening programs, is the United States Visitor and Immigration Status Indicator Technology (US-VISIT) program that uses both biometric (i.e., fingerprint, facial recognition, etc.) and biographical identification (i.e., passport, travel visa, etc.) data to document those entering the U.S. These data are catalogued in a visitor database and checked against international and domestic records of known or wanted criminals or terrorists. Ultimately, the stated goal is to create a comprehensive database of documented foreign visitors to assist in identifying fugitive or watchlist suspect entry into the U.S.

Use of Police Surveillance Technology Programs

The police themselves are placing greater emphasis on the use of technology to conduct counter-terrorism and crime investigations (Davis, 2004). As an example, the proposed 2006 budget for the Department of Homeland Security requested $51.3 million to upgrade electronic surveillance components of the "America's Shield" program (Department of Homeland Security, 2005).

As part of the mandates of the Enhanced Border Security Act (2002), federal police agencies are experimenting with the use of Radio Frequency Identification Device technology (RFID) in an effort to improve surveillance and facilitate access to biographical information on individuals. Biographical or other data can be imbedded in travel documents, identification cards, driver licenses, etc. allowing the information to be quickly accessed by radio frequency scanners. After a U.S. Government Accountability Office report (Government Accountability Office, 2005) cited a significant risk of security breaches through use of remote scanners, several federal

agencies, including police, delayed RFID implementation in some travel document and border situations. However, the technology is considered a viable surveillance and data retrieval tool and plans are underway to use it in other police applications (Davis, 2004).

Another surveillance technology being used by the police in border protection is the Unmanned Aerial Vehicle (UAV). Designed primarily for military applications, these unmanned drones are being used by the U.S. Department of Homeland Security and the U.S. Coast Guard to conduct aerial surveillance of perimeter and border regions (Fairbank, 2005). The stated purpose is to increase electronic monitoring and surveillance capability across a broad span of territory to detect illegal border crossings. Reports have shown that the UAV efficacy remains uncertain and border apprehensions have declined by 50 percent, since 2000, during the period of drone use along U.S. territorial borders (Electronic Privacy Information Center, 2005a).

Other technologies are being used to presumably improve the efficacy of police crime prevention and investigation. As seen in the aftermath of the London transit bombings in July 2005, closed circuit television (CCTV) data proved to be a viable source of information in the investigation. Like their counterparts in Britain, U.S. police are increasingly adopting the use of public area electronic surveillance to combat crime and gather information (Collins, 2005).

Police surveillance can not only affect the lives of those being watched, but also their personal information, in a number of ways. As American police widened their surveillance activities after 9/11, it has commensurate legal, political, social, and psychological effects on the civil lives of the public.

Effects of Increased Police Surveillance on Civil Life

A public perception of risk, as in the case of fear of crime, can produce effects such as increased anxiety, avoidance of public conveyances, avoidance of crowds, and increased suspicion of others. Police response to perceived threats, including increased surveillance, can act to amplify these public reactions.

Police surveillance activities are performed in two primary modes? conspicuous and inconspicuous. The more the public is aware of the police surveillance, the greater likelihood that it will affect public behaviors. However in the absence of confinement or tangible boundaries (i.e., total institution), much of the new police surveillance occurs vis-à-vis electronic media (i.e., "dataveillance, biometric, virtual identity, etc.) (Simon, 2005:1; Goffman, 1961).

Conspicuous U.S. preventive police measures can affect the public threat perception through the issuance of color-coded threat warnings, presence of heavily armed police or military in public places, and visible use of electronic surveillance devices. (Laqueur, 1999; Parenti, 2003). Conversely, as seen with several of the applications allowed by the Patriot Act, many police surveillance methods remain inconspicuous until the police decide to take enforcement action against the target of an investigation.

Three categories of potential effects of surveillance on civil life are examined here. First, one of the most identifiable consequences of increased surveillance has been the creation of new privacy boundaries that have reduced earlier safeguards. Second, are the behavioral effects that result from suspicion and the disruption of public activities? Third, is the effect brought about by a public perception of ubiquitous police surveillance?

Diminution of Privacy Rights

The first result of escalating police surveillance authority is the diminution of civil privacy protection. Essentially, an inverse relationship exists between the two, whereby, as U.S. police surveillance power grows individual privacy declines (Bloss, 1996). Legal and procedural changes have facilitated a widened of police surveillance and search resulting in more citizens being watched by officials who are collecting data on their physical and electronic selves (i.e., expression, personal data, virtual identity, and biometric identity) (see O'Harrow, 2005; EPIC, 2006). Therefore, the identities, transactions, and movements of citizens are less private and more accessible to police through burgeoning databases of personal information; all derived from official surveillance and search activities.

Specifically, established U.S. constitutional privacy protections have been diluted through post-9/11 federal statutory provisions and court decisions. Once strict requirements such mandatory judicial review, warrant and probable cause requirements, and primacy of citizen privacy, all designed to constrain police surveillance and search, have been supplanted by non-judicial intervention, warrant exceptions, and relaxed legal standards allowing the police to engage in surveillance and search with fewer restrictions. The result is the creation of a new privacy paradigm where the perception of increased public safety threat has shifted the balance away from previous citizen protections leading to a reinterpretation of the meaning of individual privacy in the post-9/11 context.

Amplifying Suspicion and Disrupting Civil Life

As noted, post-9/11 expansion of police surveillance powers is, in part, a result of an official reaction to the perception of terrorism threats. This response contributes to the second effect of police conspicuous surveillance which is to disrupt lives and alter the public perception of risk through visible preventive measures and public safety rhetoric. As Parenti (2003: 200) explains "[9/11] radically accelerated momentum toward the soft cage of a surveillance society, just as it gave the culture of fear a rejuvenating jolt."

The desire by extremists to cause disruption and promote public anxiety is among the bedrock principles of terrorism (Crenshaw, 2003). Additionally, terrorists strive to provoke an official response, which changes the stability of everyday life, through the use of symbolic political violence (See generally White, 2006). As Stohl (2003: 85) commented "[Osama] bin Laden's interviews in May 2001 with the Arab journalists also indicated that he was hoping for an unrestrained U.S. government response that would clamp down on the domestic public and limit civil liberties and "normal" American life [after the 9/11 attacks]." In this sense, both the intentional actions of terrorists, and subsequent official reactions, have led to greater public

anxiety and suspicion.

Increased public suspicion manifests itself in several ways. Public safety concerns have fueled an *alien conspiracy* reaction where immigrants and minorities are viewed with greater suspicion (Musto, 1973). In what Parenti (2003: 204) refers to as an "enemy kulturkampf," citizen mistrust of others is amplified by official rhetoric where the public is encouraged to "place all trust in unlimited state and corporate power." Romero (2003) argues that heightened anxiety about transnational terrorist threats has caused the American public to complacently relinquish civil liberties to government officials believing that they will be safer. Nowhere is this better illustrated than in the public support, or tolerance, for an expansion of police surveillance powers (Whitehead and Aden, 2002).

In the U.S. there is considerable debate about the merits of surrendering privacy rights and civil liberties for greater public safety (Chang, 2003; Whitaker, 2003; Bailey, 2004; O'Harrow, 2005; Sykes, 1999). To what extent, though, do these perceived threats promote the level of public panic desired by extremists? In addressing the *new terrorism*, Laqueur (1999: 272) suggested that public panic responses to threats of terrorism have profound effects on public life. He stated "True panic is contagious, a crowd phenomenon, not an individual one. The consequences of mass panic in both material and human terms can be huge; they can lead to a paralysis of normal life, epidemics, post-traumatic stress, and tremendous anxiety, especially if the nature and extent of the danger remains unknown."

Another area of public disruption is the impediment to free movement brought on by increased security measures. Efforts to thwart future terrorist attacks have led U.S. police to dramatically increase their preventive security measures in public places. The use of checkpoints and baggage searches in public venues has become common symbols of a greater threat perception. Though perhaps a mere inconvenience to some it has disrupted aspects of public life.

Creation of an Orwellian Surveillance State?

The third effect of additional police surveillance is the perception of an Orwellian state; that is, creating a public sense of ubiquitous official monitoring (Rosen, 2000). Some scholars, after 9/11, have issued ominous warnings that portend a chilling effect on the quality of civil life from escalating police surveillance (Romero, 2003; Whitaker, 2003). More than twenty years ago Albanese (1984) sought to analyze the privacy effects of a predicted Orwellian surveillance state. More recently, O'Harrow (2005) described a menacing personal privacy hazard posed by prolific identity thieves and overzealous government investigators who cultivated a dearth of personal data from commercial databases. Others have mentioned security measures that include national identification cards and holistic data collection (i.e., biographical, transactional, and biometric data) programs such as the U.S. Department of Defense proposed "Total Information Awareness" project (Parenti, 2003; EPIC, 2006). To some, these measures are reminiscent of methods used by twentieth century totalitarian regimes as extreme measures of social control. To others the expansion of police surveillance is an indication of the demise of fundamental democratic ideals (Chang, 2003). Given the recent upsurge in privacy and surveillance discourse in the scholarly and popular literature, many have expressed concerns about an emerging Orwellian surveillance society where personal privacy is a casualty of the counter-

terrorism campaign (Whitaker, 2003).

All together, expanding police surveillance activities have impacted civil life. Albeit framed in legal practices, these surveillance methods have affected the fragile balance between official authority and civil liberty. And they have exerted an influence on aspects of public life by raising the potential for alterations in public risk perception, anxiety, or personal decision making about public activities.

Conclusion

The post-9/11 era has brought numerous changes in the tri-part relationship between global crime and terrorism threats, U.S. citizens, and their police. At the same time, the U.S. has changed in terms of the influences of advanced technology and globalization effects on these relationships. Taken together, the conditions have produced a myriad of legal, political, social, and psychological effects on the American public stemming from escalating police surveillance. At the core, what has resulted is a far-reaching reassessment of the balance between police surveillance authority and individual privacy rights.

Current U.S. legal jurisprudence provides empirical evidence of the changing balance of competing interests between police surveillance demands and privacy safeguards (Chang, 2003). This paper has described these changes and the legal and political causes for the shifting doctrine. Yet, civil lives involve more than the legal self. Here, some of the effects of escalating police surveillance on American civil life have been discussed. However, there is an absence of understanding, among researchers, about the scope of police surveillance effects on this dimension of public existence. Much more research needs to be conducted to assess the social and psychological impact of U.S. police surveillance on civil life.

As U.S. lawmakers, courts, and policymakers react to perceived crime and terrorism threats, their actions will produce additional and unforeseen effects on the quality of privacy and civil life in society. Since legal privacy rights emanate from U.S. jurisprudence, their status can be monitored through statutory law and court decisions. Historically, these doctrines are constantly evolving and scholars should continue to monitor their changes as the dimensions of individual privacy are transformed. However, more empirical research is needed to measure the effects of U.S. police surveillance on the quality of public life, as manifested through individual decision making and psycho-social reactions.

Privacy advocates rightly warn against the diminution of individual privacy safeguards (see Sykes, 1999; Whitaker, 2003; Bailey, 2004; O'Harrow, 2005). As police surveillance continues to escalate after 9/11, its effect on safety, civil liberties, and civil lives must be carefully considered to ensure that longstanding democratic ideals are protected while enabling the police to maintain a safe society.

References

Abrams, N. (2005). *Anti-Terrorism and Criminal Enforcement, Second Edition*, St. Paul, MN: Thomson/West Publishing.

Albanese, J. (1984) *Justice, Privacy, and Crime Control*, New York: University Press of America.

Andreas, P. (2002). "Transnational Crime and Economic Globalization" in M. Berdal and M. Serrano (Eds.). *Transnational Organized Crime and International Security: Business as Usual?*, pp. 37-52, Boulder, CO: Lynne Rienner Publishers.

Bailey, D. (2004). *The Open Society: Why the 21st Century Calls for More Openness-Not Less*, Washington, DC: Brassey's.

Baker, P. (2006). "Bush Set to Send Guard to Border," *The Washington Post*, May 15, 2006, p. A01, http://.washingtonpost.com. Online. Accessed 27 June 2006.

Bandow, D. (1991). "War on Drugs or War on America?," *Stanford Law and Policy Review*, Vol. 3: 242-260.

Bennett, B. (2005). "Psst! The FBI is Having Trouble on the Line," *Time*, 8/15/2005 Vol. 166, Issue 7, p. 20.

Berdal, M. and M. Serrano (2002). *Transnational Organized Crime and International Security: Business as Usual?* Boulder, CO: Lynne Rienner.

Bloss, W. (2006). *Transnational Crime and Terrorism in a Global Context*, Boston: McGraw-Hill Publishers.

Bloss, W. (2005). "Parameters of U.S. Police Investigative Powers in a New Privacy Paradigm," *unpublished paper* presented at the 12th International Police Executive Symposium, Prague, the Czech Republic.

Bloss, W. (2002). "Privacy Rights of Police Officers: Dimensions of Employer Regulation," in Jeffrey Walker (ed.) *Policing and the Law*, pp. 135-172, Upper Saddle River, NJ: Prentice-Hall.

Bloss, W. (1996). *Privacy Issues Involving Law Enforcement Personnel: A Constitutional Analysis*, unpublished doctoral dissertation (available at UMI microfilms, University of Michigan), Sam Houston State University Huntsville, Texas.

Bridis, T. and J. Solomon (2006). "Police Got Phone Data from Brokers" *ABC News*, June 20, 2006, http://abcnews.go.com/Business/wireStory?.html. Online. Accessed 27 June 2006.

Brown, C. (2003). *Lost Liberties: Ashcroft and the Assault on Personal Freedom*, New York: The New Press.

Carter, D. (2004). "Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement," Washington, DC: National Institute of Justice.

Chang, N. (2003). "How Democracy Dies: The War on Our Civil Liberties," in C. Brown (ed.) *Lost Liberties: Ashcroft and the Assault on Personal Freedom*, pp. 33-51, New York: The New Press.

Collins, C. (2005). "Crime-Busting Cameras: A US-City Experiment," *The Christian Science Monitor*, June 27, 2005, http://www.csmonitor.com/2005/0627/p11s02-lihc.html. Online. Accessed 28 March 2006.

Crenshaw, M. (2003). "The Causes of Terrorism" in C. Kegley, Jr., *The New Global Terrorism: Characteristics, Causes and Controls*, pp. 92-105, Upper Saddle River, NJ: Prentice-Hall.

Davis, B. (2004). "Spy Gear: Modern Surveillance Tools Use the Newest Technology to Catch Crooks on the Sly," *Police*, Vol. 28, issue 10: 38-43.

del Carmen, R. (2004). *Criminal Procedure: Law and Practice, Sixth Edition*, Belmont, CA: Wadsworth/Thomson.

Department of Homeland Security (2005). "Budget-in-Brief Fiscal Year 2006," http://www.dhs.gov/interweb/assetlibrary/Budget_BIB-FY2006.pdf. Online. Accessed 28 March 2006.

Ducat, C. (2004). *Constitutional Interpretation, Eighth Edition*, Belmont, CA: Wadsworth/Thomson.

Electronic Privacy Information Center (2006), "The USA Patriot Act" at http://www.epic.org/privacy/terrorism/usapatriot/. Online. Accessed 20 March 2006.

Electronic Privacy Information Center (2005). http://www.epic.org/. Online. Accessed 18 March 2006.

Electronic Privacy Information Center (2005a). "EPIC Alert," Vol. 12:16 August 11, 2005. http://www.epic.org/alert/alert_vol_12.html. Online. Accessed 18 March 2006.

Fairbank, K. (2005). "Pilotless Aircraft Seen as Wave of the Future," *Dallas Morning News*, June 14, 2005.

Friedman, Thomas (2005). *The Flattening of the World: A Brief History of the 21st Century*. New York: Farrar, Strauss and Giroux.

Goffman, E. (1961). *Asylums: Essays on the Social Situation of Mental Patients and Other Inmates*, Garden City, NY: Anchor Books.

Government Accountability Office (2005). "Information Security: Radio Frequency Identification Technology in the Federal Government," Washington, DC: GAO, http://www.gao.gov/new.items/d05551.pdf. Online. Accessed 15 March 2006.

Grabosky, P. and R. Smith (1998). *Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities*, New Brunswick, NJ: Transaction Publishers.

Hoffman, B. (2004). "The Changing Face of Al Qaeda and the Global War on Terrorism," *Studies in Conflict & Terrorism*, 27:549-560.

Kegley, Jr., C. (2003). *The New Global Terrorism: Characteristics, Causes and Controls*, Upper Saddle River, NJ: Prentice-Hall.

Kerr, O. (2004). "The Fourth Amendment and New Technologies: Constitutional Myths and the Case forCaution," *Michigan Law Review* 102: 801-888.

Kugler, R. and E. Frost (2001). *The Global Century, Globalization and National Security, Volume II*, Washington: National Defense University Press.

Laqueur, W. (1999). *The New Terrorism: Fanaticism and the Arms of Mass Destruction*, New York: Oxford University Press.

Martin, S. (2006). "Note: Interpreting the Wiretap Act: Applying Ordinary Rules of 'Transit' to the Internet Context," *Cardozo Law Review* 28: 441-487.

McAninich, W. (1991). "Unreasonable Expectations: The Supreme Court and the Fourth Amendment," *Stetson Law Review*, Vol. 20:435-469.

Messner, D. (2002). "World Society-Structures and Trends" in P. Kennedy, D. Messner and F. Nuschler (eds.) *Global Trends and Global Governance*, pp. 22-64, London: Pluto Press and Development and Peace Foundation.

Musto, D. (1973). *The American Disease: Origins of Narcotics Control*, New Haven: Yale University Press.

O'Harrow, R. (2005). *No Place To Hide*, New York: Free Press.

Parenti, C. (2003). *The Soft Cage: Surveillance in America from Slavery to the War on Terror*, New York: Basic Books.

Peterson, M. (2005). "Intelligence-Led Policing: The New Intelligence Architecture," Washington, DC: Bureau of Justice Assistance.

Posner, G. (2003). *Why America Slept: The Failure to Prevent 9/11*, New York: Random House.

Reamey, G. (1992). "When 'Special Needs' Meets Probable Cause: Denying the Devil Benefit of Law," *Hastings Constitutional Law Quarterly*, Vol.19:295-316.

Reichel, P. (2005). *Handbook of Transnational Crime and Justice*, Thousand Oaks, CA: Sage Publishers.

Romero, A. (2003). "Living in Fear: How the U.S. Government's War on Terror Impacts American Lives" in C. Brown (ed.) *Lost Liberties: Ashcroft and the Assault on Personal Freedom*, pp. 112-131, New York: The New Press.

Rosen, J. (2000). *The Unwanted Gaze*, New York: Random House.

Shelley, L. (2005). "The Globalization of Crime" in M. Natarajan (Ed). *Introduction to International Criminal Justice*, pp. 3-10, Boston, MA: McGraw-Hill Publishing.

Siegel, D., van de Bunt, H. and D. Zaitch (2003). *Global Organized Crime: Trends and Developments*, London: Kluwer Academic Publishers.

Simon, B. (2005). "The Return of Panopticism: Supervision, Subjection and the New Surveillance, *Surveillance and Society* 3(1): 1-20. http://www.surveillance-and-society.org/Articles3(1)/return.pdf. Online. Accessed 28 June 2006.

Stohl, M. (2003). "The Mystery of the New Global Terrorism: Old Myths, New Realities?" in C. Kegley, Jr. (ed.) *The New Global Terrorism: Characteristics, Causes and Controls*, pp. 84-91, Upper Saddle River, NJ: Prentice-Hall.

Sykes, C. (1999). *The End of Privacy*, New York: St. Martin's Press.

Thachuk, K. (2001). "The Sinister Underbelly: Organized Crime and Terrorism" in R. Kugler and E. Frost (eds) *The Global Century, Globalization and National Security, Volume II*, pp. 743-760, Washington: National Defense University Press.

Taylor, R., Caeti, T., Loper, D. Fritsch, E. and J. Liederbach (2006). *Digital Crime and Digital Terrorism*, Upper Saddle River, NJ: Pearson/Prentice-Hall.

Whitaker, R. (2003). "After 9/11: A Surveillance State?" in C. Brown (ed.) *Lost Liberties: Ashcroft and the Assault on Personal Freedom*, pp. 52-74,New York: The New Press.

White, J. (2006). *Terrorism and Homeland Security, 5th Edition*, Thomson/Wadsworth.

Whitehead, J. and S. Aden (2002). "Forfeiting Enduring Freedom for Homeland Security: A Constitutional Analysis of the USA Patriot Act and the Justice Department's Anti-Terrorism Initiatives," *American University Law Review*, Vol. 51: 1081-1133.

Williams, P. (1999). "Getting Reach and Getting Even: Transnational Threats in the Twenty-First Century" in S. Eistein and M. Amir (Eds.), *Organized Crime: Uncertainties and Dilemmas*, Chicago: University of Chicago Press.

Williams, P. and E. Savona (1996). *The United Nations and Transnational Organized Crime*, London: Frank Cass.

Cases Cited

Katz v. United States, 389 U.S. 347 (1967).

Olmstead v. United States, 277 U.S. 438 (1928).

O'Connor v. Ortega, 480 U.S. 709 (1987).

Legislation Cited

Communications Assistance for Law Enforcement Act of 1994 (Digital Telephony Act).

Electronic Communications Privacy Act of 1986.

Enhanced Border Security Act of 2002.

Omnibus Crime Control and Safe Streets Act of 1968.

United States Constitution, Amendment IV.

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA Patriot Act).