TELECOMMUNICATIONS AS A WEAPON IN THE WAR OF MODERN ORGANIZED CRIME

Christopher A. Nolin†

I. INTRODUCTION AND OVERVIEW

From the advent of large scale drug trafficking operations, law enforcement has struggled to keep pace with the methods and technologies utilized by the criminal groups orchestrating them. Major Italian crime bosses successfully operated such a drug trafficking enterprise in the mid-twentieth century.[1] In 1947, eight months after being pardoned by New York Governor Thomas E. Dewey and exiled to Italy, Italian crime syndicate and Mafia boss Charles "Lucky" Luciano traveled to Havana, Cuba. There, he called a meeting of the American "godfathers," where they discussed their role in the burgeoning global market of drug trafficking.[2] Luciano and the leaders of the Italian crime syndicate developed a heroin pipeline, which featured the import of raw opium from Turkey into processing centers in Lebanon, refinement in laboratories in Italy, and subsequent distribution in America through Cuba and other nearby countries.[3] In the decades following World War II, the Italian crime syndicate exerted a stranglehold on the trafficking of heroin in the United States.[4] In Sicily, Luciano orchestrated

† J.D. Candidate, May 2007, The Catholic University of America, Columbus School of Law. Special thanks to my parents, Pat and Mike Nolin, for their constant encouragement and support of my writing. Thanks also to my friends and the CommLaw staff for being patient with me throughout the writing and editorial process.

1 ROBERT J. KELLY, ENCYCLOPEDIA OF ORGANIZED CRIME IN THE UNITED STATES 16-17 (2000). The 1957 Apalachin meeting in upstate New York was the first time a nationwide mafia conspiracy was uncovered. Prior to that date, the Mafia Commission had met every five years since 1931, with no impediment from law enforcement. *Id*

2 *Id.* at 201.

3 ALFRED W. MCCOY, THE POLITICS OF HEROIN 39 (1991).

4 KELLY, *supra* note 1, at 101. In 1964, the Bureau of Narcotics determined that the Italian crime syndicate regulated ninety-five percent of the domestic heroin trafficking ited States in the post-war years. *Id.* This was a result of Luciano peacefully solidifying the New York mobsters into five crime families, which coordinated joint trafficking ventures. The

clandestine operations to smuggle a significant supply of heroin into the United States in packages of fruits, vegetables or candy.[5] The contraband was often distributed through Mafia-owned businesses, such as pizza parlors, in large American cities.[6]

In the 1970s, the struggle for power between Italian crime families in the United States ceded room to other competitors in the drug trafficking industry.[7] Armed with the narcotic cocaine made from coca plants in Bolivia and Peru, Colombian drug traffickers took advantage of the situation. They created their own distribution and smuggling operations known as cartels, which oversaw the complete development of raw materials into pure narcotics ready for distribution.[8] By the mid-1980s, the Medellín and Cali cartels controlled more than half the world's cocaine supply, and infiltrated every major American city.[9] Though the face of the traditional drug trafficking organization changed considerably in the United States, the way in which the South American crime cartels controlled prices, hid and laundered profits, and perpetuated corruption[10] evokes the power of Italian drug trafficking "dons."

This Comment will explore the role played by modern advancements in telecommunications in dictating the operations of drug traffickers and the impact of telecommunications legislation intended to combat these operations. It will begin with a discussion of the structural evolution of modern drug trafficking, highlighting the organization of the Colombian pioneers of the most notorious cocaine trafficking organizations, especially in comparison to their Italian predecessors. While the Italian drug operations pri-

---

same five Italian crime families still exist today. PATRICK J. RYAN, ORGANIZED CRIME 41–42 (1995).

[5] MCCOY, *supra* note 3, at 39. Luciano's heroin refinement laboratories in Sicily often operated under the guise of candy factories. *Id.*

[6] KELLY, *supra* note 1, at 241–42.

[7] *See id.* at 72–73.

[8] *Id.* Farmers in Bolivia and Peru transferred coca plants to vast laboratories in the Colombian jungles, where they processed them into cocaine and sent the product out for transport. *Id.* Deep in the remote jungles of southern Colombia, drug traffickers set up massive laboratories to process cocaine. One such drug lab was called "Tranquilandia" due to its isolation, and it thrived undetected by law enforcement despite producing approximately $15 billion of cocaine in the early 1980s. *Frontline: Drug Wars* (PBS television broadcast Oct. 9, 2000) [hereinafter *Frontline: Drug Wars Television Broadcast Transcript*], *available at* http://www.pbs.org/wgbh/pages/frontline/shows/drugs/etc/script.html. The DEA thought it had turned a corner on drug trafficking enforcement with the publicized bust of Tranquilandia on March 10, 1984. The impact on the trafficking industry, however, was minimal; the seizure did not affect availability or purity because several immense cocaine laboratories remained in the Colombian jungles. *Id.*

[9] KELLY, *supra* note 1, at 72.

[10] *Id.* at 73. Specifically, Colombian cartel members engaged in corrupt politics, covertly supplying security or narcotics for elected officials and law enforcement, and more publicly eliminating those officials who targeted drug trafficking organizations. *See* RYAN, *supra* note 4, at 52–53.

marily depended on the concerted efforts of individuals to smuggle manufactured heroin into the United States, modern drug trafficking organizations have huge infrastructures. In these organizations, hundreds of cartel agents must have the ability to communicate with all other facets of the cartel in order to carry out their specific roles. For years the drug trafficking sector of the Italian crime syndicate went undetected by U.S. law enforcement officials, who refused even to recognize the syndicate.[11] During the United States' "War on Drugs," however, significant law enforcement resources were directed at minimizing drug infiltration into American cities and the social damage caused by the Latin American cartels. As a result, these drug trafficking organizations were forced to adopt more evasive smuggling techniques to circumvent prosecution. They developed sophisticated methods of communication to avoid initial detection. Part III of this Comment examines the evolution of communications practices utilized by major drug trafficking organizations in the modern age of telecommunications advancements. This part first documents the transition from analog to a digital cellular age over the recent decades. Then, it assesses law enforcement's ability to adjust to this changing technological landscape and its struggles to keep pace in the collection of evidence for criminal investigations in the face of innovative and illicit use of telecommunications devices and channels.

In Part IV, this Comment examines the laws Congress has enacted to enable United States law enforcement to conduct electronic wire surveillance of telecommunications between syndicate agents. Specifically, this Comment explains that Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Omnibus Act")[12] is particularly effective in balancing the government's law enforcement interests with Fourth Amendment privacy issues. Next, this Comment discusses the ongoing attempts to adapt surveillance techniques under Title III to keep pace with drug trafficking organizations and their use of modern innovations in telecommunications. This discussion focuses on the Communications Assistance for Law Enforcement Act of 1994 ("CALEA"),[13] which demands the cooperation of major telecommunications networks to permit more widespread access to electronic surveillance channels. This Comment will argue that CALEA must be modified to require full compliance by telecommunications carriers if it is to be completely effective in combating drug trafficking in the coming years.

---

[11] KELLY, *supra* note 1, at 17. The 1957 Apalachin meeting forced J. Edgar Hoover to take action against this national criminal conspiracy. *Id.*

[12] Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90–351, 82 Stat. 197 (1968).

[13] Communications Assistance for Law Enforcement Act, Pub. L. No. 103–414, 108 Stat. 4279 (1994).

Finally, Part V of this Comment ponders the impact of extensive surveillance on the American people in the midst of a "War on Terror," and suggests that CALEA and the Omnibus Act serve as examples of how the legislation regarding electronic surveillance effectively balances robust law enforcement while protecting individual constitutional rights.

II. THE NEW MAFIA: THE CRIMINAL DRUG TRAFFICKING SYNDICATE

A. Structural Evolution of the Modern Drug Trafficking Industry

Compared to Italian and Colombian drug trafficking organizations of the past, modern drug trafficking organizations are more complex. Like the Sicilian heroin refinement workers and smugglers employed by the Italian drug trafficking syndicate in the 1950s and 1960s, the key forces behind the development of prominent Colombian drug cartels in the 1970s were Colombian nationals, often related to one another.[14] Modern drug trafficking organizations demand an enormous infrastructure, with hundreds of individual agents, called "cells." These cells facilitate different facets of the operation, ranging from narcotic cultivation and distribution to the cartel's business management.[15] In their home countries, these drug trafficking enterprises also rely on the aid of corrupt politicians and law enforcement officials, who often turn a blind eye because they receive payoffs or are threatened with assassination.[16]

A look into the evolution of the Colombian drug cartels, with specific attention paid to the Medellín and Cali cartels, reveals a complex framework underpinning this primary vehicle for organized crime in the Americas in

---

[14] KELLY, *supra* note 1, at 73. "For bloodlines and kinship, the Colombian gangs match those of Sicily." RYAN, *supra* note 4, at 52. The Ochoa brothers, Jorge, Juan David and Fabio, were sons of respected Colombian ranchers who became three of the founders of the Medellín cartel, a notorious Colombian cocaine trafficking enterprise. *See Frontline: Drug Wars, The Business: Colombian Traffickers*, *available at* http://www.pbs.org/wgbh/pages/frontline/shows/drugs/business/inside/colombian.html [hereinafter *Drug Wars: Colombian Traffickers*].

[15] KELLY, *supra* note 1, at 73. Cartels employ thousands of Colombians and interact with thousands more in the United States, often indirectly. Those who deal directly with cocaine include farmers who grow coca plants in Bolivia, Peru, and more recently, Columbia, to distributors and street dealers in the United States. Those who manage the business aspects of the cartel include accountants, and lawyers, and chemists who process the drugs. *Id.*

[16] *See id.* Similar to the Italian Mafia, the Colombian cartel members frequently became involved in corrupt politics, whether providing protection or narcotics for officials, or violently eliminating opposing politicians. *See* RYAN, *supra* note 4, at 52. See *infra* note 18 for an overview of the fickle relationship between Medellín kingpin Pablo Escobar and the Colombian political system.

the past several decades, and the foundation of a thirty-year war on drugs.[17] The Medellín cartel rose to power in Colombia in the 1980s, capitalizing on the demand for cocaine in the United States and other parts of South America. The Medellín was tremendously profitable because of the returns it received on investments in its narcotics manufacturing labs. Violent drug lords Pablo Escobar and the Ochoa brothers powerfully led narcotics manufacturing and smuggling operations.[18] Additionally, the Medellín cartel cultivated social acceptance and public support through its public works and community social programs.[19]

The Cali cartel ("Cali"), named after the city in Colombia in which it was based, employed organizational methods more consistent with the Italian crime syndicate. Unlike the efforts of their Medellín counterparts, Cali's smuggling operations were covert and designed to evade prosecution and opposition.[20] Not unlike the Italian drug trafficking organizations,

---

[17] *See Drug Wars: Colombian Traffickers, supra* note 14.

[18] *See Frontline: Drug Wars Television Broadcast Transcript, supra* note 8. Escobar and the Medellín effectively operated under the nose of Colombian law enforcement because Escobar's soldiers threatened police, government officials, prosecutors, judges, journalists, and even innocent bystanders with violent execution. *Id.* at 25. In 1976, Escobar was arrested when Columbian law enforcement agents found thirty-nine kilos of cocaine in his truck. When Escobar's attempt to bribe the judge failed, he blackmailed the judge by retaining his brother as counsel. MARK BOWDEN, KILLING PABLO 24 (2001). After the judge recused himself and while the retrial was tied up in the appeals process, Escobar had the two agents responsible for the arrest killed. *Id.* The violence and corruption continued when Rodrigo Lara was appointed Colombian justice minister in 1983. He mounted a campaign of investigations into Escobar's past drug activities and succeeded in getting Escobar kicked out of office, which lifted his parliamentary immunity. *Id.* at 40. Three months later, Lara was murdered in Bogotá. *Id.* at 41. A final illustration of Escobar's brutality and control can be seen in the fickle manner in which he dealt with the media. When faced with legal trouble, Escobar used the media to his advantage by transmitting messages to stir up public support. When he was derided by the media, however, he would have reporters and editors executed. *Id.* at 241.

[19] Escobar, for instance, established himself as a modern-day Robin Hood. *Frontline: Drug Wars Television Broadcast Transcript, supra* note 8. Escobar spent millions on improvements to city slums, donating funds, building roads and roller-skating rinks, and lighting soccer fields. Additionally, he started a housing development for the poor and homeless. The community took notice of Escobar's philanthropy. Besides being "the richest and most powerful man in Antioquia; he was also its most popular citizen." BOWDEN, *supra* note 18, at 28–29. "The whole nation wanted to join Pablo's party." *Id.* at 24.

[20] *Drug Wars: Colombian Traffickers, supra* note 14. Cali management realized that drug trafficking operations were more profitable when executed covertly, undetected by Colombian and United States law enforcement and prosecution. Accordingly, kingpins received briefings from prominent international lawyers who were hired to study the tactics of the Drug Enforcement Administration ("DEA") and United States law enforcement. The Cali drug lords also hired and trained technological engineers to develop communications equipment which would avoid detection and interception by law enforcement. *Id.* The Medellín cartel also benefited from advanced intelligence that rivaled that of the DEA, and thus reduced the DEA's threat to the narcotics organization. *Frontline: Drug Wars Television Broadcast Transcript, supra* note 8.

Cali engaged and invested in legitimate business as a front for their drug trafficking operations.[21] Both the Cali and Medellín cartels had agents and connections in Colombian law enforcement and politics,[22] enabling them to receive favors and further evade prosecution in their own endeavors.[23]

In the late 1990s, Mexico-based criminal organizations joined the drug trafficking community by collaborating with Colombian cartels as cocaine transporters and wholesale-level distributors.[24] Today, Mexican criminal groups exert more influence over drug trafficking than any other narcotics organization, and Colombian cartels continue to rely on Mexican drug organizations for the transportation and smuggling of narcotics into the United States.[25] The narcotics are smuggled into the United States by

---

[21] *See Drug Wars: Colombian Traffickers, supra* note 14. See *supra* text accompanying note 5 for a comparison of Cali's Italian counterpart in drug trafficking. The Medellín cartels amassed hundreds of millions of dollars each year and used the profits to expand their cultivation and trafficking operations or outside business investments. *Frontline: Drug Wars Television Broadcast Transcript, supra* note 8. What made this trade even more lucrative for the Medellín was the fact that the Colombian government encouraged the creation of funds in business markets with extremely high interest rates. Thus, investors in "legitimate" government funds were in effect "cash[ing] in on the drug bonanza" in Colombia. BOWDEN, *supra* note 18, at 25.

[22] *See Drug Wars: Colombian Traffickers, supra* note 14. Medellín kingpin Pablo Escobar immediately infiltrated Colombian politics with his election to the city council in 1978 and then to the position of National Congressman in 1982. This title conferred automatic judicial immunity; thus, in addition to contributing to the lawmaking process, Escobar was also above the law and free from prosecution. BOWDEN, *supra* note 18, at 30–31. Such corruption was not limited to the Colombia political arena; in the early 1980s, the Medellín cartel included Prime Minister Norman Pindling of the Bahamas on their underground payroll. Pindling offered his more deserted islands as an intermediate base for traffickers to organize and consolidate cocaine for conversion into shuttle aircrafts headed for the United States. In exchange for pay-offs and kickbacks, Pindling further facilitated the success of Colombian cartels in the Bahamas by laundering money and business investments. *Frontline: Drug Wars Television Broadcast Transcript, supra* note 8.

[23] *Drug Wars: Colombian Traffickers, supra* note 14. The Cali cartel gained preferential treatment from the Colombian police as well as American law enforcement organizations such as the DEA by providing information concerning their nemesis, Pablo Escobar and the Medellín. *Id.*

[24] *See* DEA BRIEFS & BACKGROUND, DRUGS AND DRUG ABUSE, DRUG DESCRIPTIONS, DRUG TRAFFICKING IN THE UNITED STATES 2, http://www.usdoj.gov/dea/concern/drug_traffickingp.html [hereinafter DRUG TRAFFICKING IN THE UNITED STATES]. These were not the only two groups to join forces. In 1994, the "Project Onig" investigation targeted a massive drug trafficking network involving Italian organized crime and Colombian drug cartels. *In re* Communications Assistance for Law Enforcement Act, *Declaration of FBI Director Louis J. Freeh*, CC Docket No. 97-213, 10 (Jan. 27, 1999) [hereinafter *Freeh Declaration*] (accessible via FCC Electronic Comment Filing System).

[25] DEP'T OF JUSTICE, NAT'L DRUG THREAT ASSESSMENT 2005: THREAT MATRIX (2005), http://www.usdoj.gov/ndic/pubs11/13817/13817p.pdfx. Mexico produces and smuggles into the United States much of the marijuana and methamphetamine found in American drug markets. *Id.*

land,[26] air[27] and water.[28] They are then distributed in major metropolitan areas throughout the country.[29]

Managing an international empire of narcotics manufacturing and distribution is a monumental task for the drug kingpin or cartel manager. Like the Italian crime bosses that came before him, the drug kingpin is responsible for making strategic decisions and issuing direction to his virtual army of agents. The most significant difference from his Mafia predecessors is that the kingpin always directs operations from foreign soil.[30] Numerous transactions are carried out simultaneously and the kingpin must have seamless communications with his cells.[31] Effective coordination of the enterprise requires accurate transmission of information to international cells regarding warehousing locations for loads of narcotics, contacts for providing transportation once the narcotics arrive at a destination, and locations for delivering the profits.[32]

The benefits of a widespread infrastructure for cells to effectively communicate information with each other is compounded by the United States' combative approach in recent decades towards South American drug trafficking. President Richard Nixon first launched the "War on Drugs"[33] in

---

[26] DRUG TRAFFICKING IN THE UNITED STATES, *supra* note 24, at 2. The Medellín and Cali Colombian cartels possess their own fleets of boats and aircrafts. The United States–Mexico border is the main point of entry for cocaine smuggled into the United States; a majority of it crosses the Southwest border, brought in by illegal aliens. *Id.*

[27] Pablo Escobar went from stuffing ten thousand kilos of cocaine into small planes to using stripped Boeing 727s for international narcotics smuggling. BOWDEN, *supra* note 18, at 34. Small, twin-engine aircrafts were the inconspicuous means of choice for Colombian drug traffickers. Over the course of one month, six flights could deliver up to two thousand kilos of cocaine, worth approximately $100 million. *Frontline: Drug Wars Television Broadcast Transcript*, *supra* note 8.

[28] Escobar even built small, remote-controlled submarines to send up to two thousand kilos of cocaine to the waters off the coast of Puerto Rico. Divers then recovered the delivery and transferred it to Miami in cartel-owned speedboats. BOWDEN, *supra* note 18, at 34.

[29] *See* DRUG TRAFFICKING IN THE UNITED STATES, *supra* note 24, at 2. Cities under the control of Mexico-based trafficking groups for cocaine distribution include Chicago, Dallas, Denver, Houston, Los Angeles, Phoenix, San Diego, San Francisco, Seattle, and more recently, Atlanta. Colombian-based cocaine distribution is prominent in cities along the eastern seaboard such as Boston, New York, Newark, Philadelphia, and Miami. *Id.*

[30] *See Clone Phones: Hearing Before the H. Comm. on the Judiciary, Subcomm. on Crime*, 104th Cong. 11 (1997) [hereinafter *Cellular Phone Fraud Hearing*] (statement of Anthony R. Bocchichio, Asst. Admin. for Operational Support, DEA). "Traditional organized crime leaders operating in places like New York, Chicago or Las Vegas called their business shots on American soil." *Id.*

[31] *See id.*

[32] *Id.*

[33] Debate, *The War on Drugs: Fighting Crime or Wasting Time?*, 38 AM. CRIM. L. REV. 1537, 1539 (2001). At a press conference shortly after his inauguration in 1971, President Nixon called drug abuse "public enemy number one in the United States," and determined it was "necessary to wage a new all-out offensive." *Id.* Many states implemented severe drug laws; New York's "Rockefeller Laws" featured harsh sentences for drug offenders. *Id.* The Nixon administration devoted more resources to drug treatment than law enforcement.

1971, targeting the spread of narcotics on a domestic level, while aiming to reduce the influx and supply of narcotics from drug-producing countries.[34] President George H.W. Bush advanced this policy by invading Panama with American troops to capture kingpin and Army General Manuel Noriega, who surrendered to the DEA in January of 1990.[35] Never considered victorious,[36] the War on Drugs continues.[37] Despite American efforts

---

Frontline: Drug Wars Television Broadcast Transcript, *supra* note 8. Under Nixon's "total war" against "the problem of dangerous drugs," federal spending went from $80 million to over $600 million in just his first term. *Id.* His legacy in the War on Drugs exists in the 1973 creation of the DEA. *See id.* Although President Reagan did not consider domestic drug abuse a more pressing issue than foreign policy when he took the White House in 1981, he agreed that drug abuse remained "one of the gravest problems" affecting the United States. *Id.* To attack this problem, Reagan gradually adopted a harsh policy of interdiction. Aside from Nancy Reagan's "Just Say No" social campaign directed towards the middle class youth, the DEA formed anti-drug units like the South Florida Drug Task Force, designed to seize and destroy narcotics in high-traffic areas such as Miami. *Id.* The cost of such federal law enforcement interdiction efforts under Reagan surpassed $1 billion. *Id.* The signing of the Anti-Drug Abuse Acts of 1986 and 1988, which are best known for mandatory minimum sentences for drug offenders, illustrates Reagan's imprint on the drug wars in America. See *The War on Drugs: Fighting Crime or Wasting Time?*, *supra* note 34 at 1539. This hard-line stance continued under President George H.W. Bush, who named the War on Drugs his top domestic policy priority. He created the Office of National Drug Control Policy in 1989, headed by the "Drug Czar," and increased military spending for drug enforcement by fifty percent. *Id.* President Clinton continued the military focus of the War on Drugs, appointing retired Army General Barry McCaffrey to the position of Drug Czar. In August of 2000, Clinton authorized and delivered $1.3 billion in United States aid to Colombia to fund combat helicopters and training of the Colombian military as part of "Plan Colombia." *Frontline: Drug Wars, Thirty Years of America's Drug War: A Chronology*, http://www.pbs.org/wgbh/pages/frontline/shows/drugs/cron [hereinafter *Drug Wars: Chronology*].

[34] Kyle Grayson, *Discourse, Identity, and the U.S. 'War on Drugs,' in* CRITICAL REFLECTIONS ON TRANSNATIONAL ORGANIZED CRIME, MONEY LAUNDERING, AND CORRUPTION 151–52 (Margaret E. Beare ed., 2003). Domestically, the "fashionable" drug cocaine was targeted, and drug penalties for dealers and consumers were increased. Internationally, the DEA identified certain nations as drug producers and traffickers, and the United States donated military equipment to fight the cartels. The War on Drugs allowed for military involvement in civilian law enforcement. *Id.*

[35] *Drug Wars: Chronology*, *supra* note 33. Noriega was convicted on charges of drug trafficking, money laundering and racketeering and was sentenced to forty years in United States federal prison. Noriega conspired with the Colombian Medellín cartel and allowed them to launder money and invest in enormous cocaine laboratories in Panama. *Id.* Noriega was a "friend of the cartel people," and offered asylum to Escobar and the Ochoa brothers when Colombian President Belisario Betancur sought to extradite the Medellín kingpins following the assassination of Rodrigo Lara Bonilla, the top Colombian judicial official, on Apr. 30, 1984. *Frontline: Drug Wars, Interviews*, http://www.pbs.org/wgbh/pages/frontline/shows/drugs/interviews/arenas.html (interviewing Fernando Arenas, pilot for Medellín kingpin Carlos Lehder).

[36] *See Frontline: Drug Wars, Statistics and Charts*, http://www.pbs.org/wgbh/pages/frontline/shows/drugs/charts/ (last visited Oct. 28, 2006). By the year 2000, more than sixty percent of federal inmates were serving sentences for drug offenses. Compare this to sixteen percent of federal inmates in 1970, and twenty-four

to stem the domestic manufacture and distribution of narcotics, the Colombian drug cartels will persist so long as their nation's economy heavily relies on its drug trafficking industry, which will continue as long as cartels are permitted to pursue all avenues to perpetuate this lucrative business.[38]

B. Use of Advanced Communications in Evading Scrutiny by American Law Enforcement

The economic efficiency of drug trafficking organizations stems largely from the historical success that Colombian kingpins have had in identifying and implementing advanced technologies for effective communication within the cartel.[39] The attention and scrutiny that leaders of the War on Drugs have invested in crippling the efforts of drug trafficking organizations in recent decades have forced the cartels and other drug smuggling organizations to rely heavily on telecommunications to coordinate their illicit operations in order to avoid law enforcement detection and prosecution.[40] For example, from the 1980s to early 1990s, Colombian cartels used pagers, creating codeword systems to convey times and locations for transactions.[41] Pay phones provided a virtually untraceable medium when live voice communication was required.[42] In the mid- to late-1990s, phone arcades, pre-paid phone cards, and faxes became popular methods of message transmission.[43] As the technology emerged, drug lords gradually in-

---

percent of federal inmates in 1980. *Id.* This illustrates one of the greatest failures of the War on Drugs: "the inability to curb the demand for drugs." Deborah Amos, *Drug Wars: All Things Considered* (Nat'l Pub. Radio radio broadcast Oct. 13, 2000), *available at* http://www.npr.org/news/specials/drugwars/atccoverage.html. Drug users are statistically more likely to end up in prison than in treatment, despite studies showing that money spent on treatment is more effective than law enforcement in reducing drug demand. *Id.*

[37] Grayson, *supra* note 34, at 153. Plan Columbia is a modern military aid package. However, it seems to perpetuate the War on Drugs by supplying military arms and aid to Colombian law enforcement, rather than providing for the reorganization and improvement of the country's social structure and economic institutions. *Id.* See discussion *supra* note 33 for a brief review of the United States' contribution to Plan Colombia.

[38] KELLY, *supra* note 1, at 76.

[39] *See Drug Wars: Colombian Traffickers, supra* note 14. Cali hired top engineers and technology experts to design sophisticated communications equipment that was undetectable by law enforcement. The Cali kingpins often pioneered innovative uses of communications technology to successfully carry out their operations. *See Cellular Phone Fraud, supra* note 30, at 11.

[40] *See Freeh Declaration, supra* note 24 ¶ 17.

[41] *Cellular Phone Fraud Hearing, supra* note 30, at 12.

[42] *Id.* Pay phones are still popular among drug traffickers today. Interview with Manuel Estrella, Spanish Translator and Wire Monitor, DEA, in Washington, D.C. (Jan. 26, 2006).

[43] *Cellular Phone Fraud Hearing, supra* note 30, at 14. Pre-paid calling cards are easily accessible and available for purchase through post offices, vending machines, and a variety of other public sites. Resembling modern Internet cafés, the term phone arcade describes the prevalent foreign shops in which private phone booths are made available for public use by paying the clerk for calls made. Calls from phone arcades tend to evade surveillance

corporated cellular phones into their operations; they bought the phones in lots and discarded them periodically to insulate themselves from surveillance.[44]

Globally, the drug trade ranks among the most serious outgrowths of organized crime.[45] In addition to those it directly affects, drug trafficking indirectly inflicts harm on society through violent acts such as kidnappings, public turf battles, and robberies committed by drug dealers.[46] Drug trafficking generates exorbitant health care expenses and devastating effects on productivity, industry, and public safety, particularly with regard to inner-city children and the unborn children of addicted mothers.[47] Given the nation's efforts in combating the War on Drugs, however, United States law enforcement remains optimistic that progressive, efficient electronic surveillance of major narcotics organizations and cartels will lead to a decline in the debilitating effects of drug trafficking and organized crime.[48] United States law enforcement agencies generally agree that electronic surveillance may be the most important and sophisticated investigative device available in the prevention, investigation, and prosecution of organized crime.[49] In the world of drug trafficking, electronic surveillance is often the only method available to intercept communications between the drug kingpin and his highest officers within the crime enterprise.[50]

---

because the caller's identity is hidden behind his cash transaction with the storefront clerk. *Id.*

[44] *Id. at 15.*

[45] It has been called "the linchpin of transnational crime." Grayson, *supra* note 34, at 145.

[46] *Freeh Declaration, supra* note 24, ¶ 17. Medellín kingpin Pablo Escobar first gained power and notoriety in 1971 when he kidnapped Diego Echavarria, a conservative factory owner who was known for mistreating the poor working class. BOWDEN, *supra* note 18, at 20–21. This act made Escobar a hero in the Medellín slums, and other such "acts of charity" contributed to the level of prominence Escobar reached in the following decades. *Id.* at 21.

[47] *Freeh Declaration, supra* note 24, ¶ 17. These societal costs are representative of organized crime, Freeh explains, and "extremely harmful to American business and industry," which additionally bears the price tag that accompanies high consumer costs, low employment, and underpayment of taxes. *Id* ¶ 15.

[48] *Id.* ¶¶ 9–10.

[49] *Id.* ¶ 9.

[50] *Id.* ¶ 18. An early example of the success of electronic surveillance is found in the events surrounding the capture and death of Pablo Escobar. By the early 1990s, Escobar was "the most wanted fugitive in the world," and American law enforcement as well as various Colombian factions wanted him dead. BOWDEN, *supra* note 18, at 237. Using a portable eavesdropping and direction-finder device given to Colombian law enforcement's electronic-surveillance unit by the Central Intelligence Agency ("CIA"), agent Hugo Martinez attempted to locate Escobar by tracking his daily phone calls from his hideout. *Id.* at 206. The device monitored the frequencies used for conversation and triangulated the target signal of the call, locating it within an area of the city. *Id.* Finally, on December 2, 1993, Colombian law enforcement agents, with the help of the CIA's surveillance device, were able to pinpoint Escobar's hideout in a two-story row house in south-central Medellín, Colombia, and Pablo Escobar was shot and killed. *Id.* at 246–49.

III. TELECOMMUNICATIONS ADVANCEMENTS

A. Transition to a Digital World Signifies a Shift in Surveillance Capacity

A brief and recent history of the telecommunications industry in the United States explains why the War on Drugs' electronic and telecommunications surveillance of drug trafficking organizations has faced considerable obstacles. Prior to 1984, American Telephone & Telegraph ("AT&T") carried a sizeable majority of the nation's local and long distance telecommunications services.[51] Because of its domination of the industry, AT&T had the advantage of employing a uniform system of equipment and analog technology.[52] Accordingly, law enforcement agents easily conducted electronic surveillance of private telephone landlines by accessing the "local loop"[53] of lines between the carrier and the private home or office.[54] AT&T's 1984 dissolution complicated the previously straightforward process for law enforcement[55] in that it gave rise to an innovative but crowded telecommunications industry with thousands of different service providers.[56] The replacement of analog technology with digital technology exacerbated this problem because computers routed calls outside of the local loop and through other communications networks.[57] Once this occurred, only the network carrier possessed the appropriate equipment to intercept the "call-identifying information"[58] needed for electronic surveillance.[59]

Traditionally, law enforcement used several methods of legally-authorized electronic surveillance to gather evidence in criminal investigations.[60] Such efforts are often directed at monitoring a suspect's operations over telecommunications lines. In order to ensure the legality of such

---

[51] *In re* Communications Assistance for Law Enforcement Act, *Declaration of Supervisory Special Agent Dave Yarbrough*, CC Docket No. 97-213, ¶ 5 (Jan. 27, 1999) [hereinafter *Yarbrough Declaration*] (accessible via FCC Electronic Comment Filing System).

[52] *Id.*

[53] Local loop refers to the connection between a telecommunications company's central office for a particular locality to the telephone or modem lines in the subscriber's home or office. *See* JONATHAN E. NUECHTERLEIN & PHILIP J. WEISER, DIGITAL CROSSROADS: AMERICAN TELECOMMUNICATIONS POLICY IN THE INTERNET AGE 33 (2005).

[54] *Yarbrough Declaration*, *supra* note 51, ¶ 6. Using a Dialed Number Recorder ("DNR"), law enforcement was able to collect the entire record of all communications and dialing information transmitted over the lines during a call, as well as the duration and status of the call. *Id.* ¶¶ 6–7.

[55] *Id.* ¶¶ *8, 11.*

[56] *Id.* ¶ 8.

[57] *Id.*

[58] 47 U.S.C. § 1001 (2000).

[59] *Yarbrough Declaration*, *supra* note 51, ¶ 11.

[60] *Id.* ¶ 3.

monitoring, law enforcement agents must, pursuant to the Omnibus Act,[61] apply for a court-authorized wire intercept of a suspect's communications occurring over specified media.[62] Having secured a warrant to intercept and install telephonic intercept hardware, the law enforcement officer may use an origin-identifying device[63] or wiretap, which monitors the actual content of the communications.[64]

B. Traffickers Capitalize on Communications Advancements to Evade Surveillance

Modern drug trafficking organizations have exploited the transition from analog to digital communications, investing heavily in the latest technological innovations in order to avoid detection. As a result, United States law enforcement agencies face an arduous task in tracking their enterprises.

1. Basic Telecommunication Methods Employed By Drug Trafficking Organizations

Agents in large and powerful cartels use payphones liberally while overseas or in foreign countries because they are typically free from electronic surveillance by law enforcement.[65] Additionally, two-way pagers allow for rapid communication and protection from possible law enforcement surveillance better suited to telephone-line communications.[66] Push-to-talk, or walkie-talkie communications, offers a quicker and more cost efficient two-way international radio connection for users.[67] Pre-paid calling cards

---

[61] Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90–351, 82 Stat. 197.

[62] *Freeh Declaration*, *supra* note 24, ¶ 2 n.1.

[63] Examples of such equipment are trap-and-trace and pen register devices. *See infra* notes 91–92 and accompanying text.

[64] *Freeh Declaration*, *supra* note 24, ¶ 2 n.1. "Wiretapping" refers to the process that uses court-ordered authorization to intercept the contents of wire or electronic communications. *Id.*

[65] Interview with Manuel Estrella, *supra* note 42. According to Mr. Estrella, the use of pre-paid phone cards among drug traffickers also has not significantly declined since the 1990s. *Id.*

[66] *Cellular Phone Fraud Hearing*, *supra* note 30, at 12. Pagers, especially two-way communicators, are safe means of communication because they allow for the use of cryptic codes to convey information such as location and strategy, rather than potentially-incriminating number and voice communication. *Id.*

[67] Elisa Batista, *"Push-to-Talk" Spreading Fast*, WIRED NEWS, Sept. 24, 2003, http://www.wired.com/news/business/0,1367,60554,00.html. Sprint and Nextel made digital cellular, two-way radio and text-numeric paging phones accessible to the general public with its "Direct Connect" service release in 1996. *Id.* Due to competition from carriers such as Verizon, which released its own push-to-talk service in August of 2003, the price for push-to-talk communications has reached a point that does not much exceed an average

also remain an effective alternative for criminals seeking to evade electronic surveillance since law enforcement can no longer intercept the "post cut-through" dialed digits.[68] Pre-paid cellular phones, a more recent innovation, are growing in popularity among drug traffickers because they are disposable and difficult to trace.[69] A drug kingpin or major cartel officer may also use a satellite phone, which provides coverage in all ocean areas, air routes, and landmasses. Though these phones are extremely expensive, calls can be made anywhere in the world;[70] and because they are typically used in conjunction with pre-paid phone cards, satellite phones are virtually impossible to trace.

Other features added to cellular phones in the past few years, including call waiting, call forwarding, conference calling, three-way calling, and call transfer, may be engaged by criminal drug traffickers to conceal incriminating conversations.[71] For example, criminals use call forwarding to redirect calls outside of the same line loop, rendering the information virtually untraceable.[72] By manipulating conference call holding features, agents may evade surveillance while coordinating criminal activities from remote locations or even prison.[73] More basic techniques can be just as difficult to trace; criminals avoid direct conversation by first employing

---

monthly cellular phone plan. *Id.* By requiring that customers subscribe to AT&T Wireless and its partner companies providing communications abroad, companies like Fastmobile Inc. have introduced instant push-to-talk communications worldwide. *Id.* In addition to push-to-talk, the service offers advanced messaging features like instant video and voice messages. *Id.*

[68] *See Yarbrough Declaration, supra* note 51, ¶¶ 49–50. Named for the intermediate carrier, usually an 800 number service that prompts the caller to continue dialing, post cut-through dialed digits were once traceable by law enforcement under the AT&T setup. *Id.*

[69] *Cellular Phone Fraud Hearing, supra* note 30, at 14. Wire monitors who are receiving a feed from a pre-paid cellular phone are able to obtain the number of the phone making the call, but unlike cellular phones from a major service, monitors are unable to tell where the calls are coming from. Interview with Manuel Estrella, *supra* note 42.

[70] Interview with Manuel Estrella, *supra* note 42. According to Mr. Estrella, the high price of these phones makes them rare, but they are growing in popularity among criminal organized crime members. *Id.*

[71] *Yarbrough Declaration, supra* note 51, ¶ 9. For example, Manuel Estrella believes that he sometimes monitors a call in which one of these procedures has been implemented, because he can only hear one side of the conversation. Interview with Manuel Estrella, *supra* note 42.

[72] *Yarbrough Declaration, supra* note 51, ¶ 10.

[73] *Id. ¶ 17.* The originator of a conference call is able to place one or more parties on hold while connecting with additional parties, and also is able to drop from the call while it continues. *Id.* ¶ 14. This poses the particular problem to law enforcement of not being able to identify or distinguish which specific criminal party was completely dropped from the conference call, or merely placed on hold during the conference call. *Id.* ¶ 17. This information is vital when law enforcement is attempting to implicate a conspirator in drug trafficking operations; law enforcement must be able to prove that a conspirator was present during the conversation and heard or made statements furthering the crime. *Freeh Declaration, supra note 24, ¶ 21.B.*

pre-established ring signals to convey messages to each other. Then, they direct incoming calls to their cellular phone's voice-mailbox, only to retrieve the messages from an outside public telephone.[74] Finally, instant messaging services are becoming a medium of choice among criminals because communication is rapid and there is no law enforcement technology to monitor the correspondence.[75]

2. Fraudulent Practices

As if the methods of otherwise legal cellular communications were not difficult enough to monitor, law enforcement surveillance of communication in a drug trafficking organization becomes extremely difficult when illegal measures such as "counterfeit fraud"[76] are put into practice. Cellular phone cloning, a type of counterfeit fraud, became very popular among technologically advanced criminal networks in the mid-1990s.[77] This procedure uses electronic wire scanners to record civilian cellular phone identification numbers, allowing the criminal to program these numbers into his own cellular phones for use.[78] The entire process takes a matter of minutes, after which the cloned cell phone, using the pirated identification numbers, can be used to make or receive calls independent of the original cellular phone.[79] A related method of counterfeit fraud is called tumbler phone-cloning, wherein the criminal stores a bulk of previously pirated cellular phone identification numbers into a phone.[80] When the criminal wishes to make a call, he cycles through any number of identification numbers, and the call goes through as if the original phone is dialing.[81] This practice thwarts traditional law enforcement intercept devices, which stop recording information when they are no longer receiving data from a specific line.[82] Finally, subscription fraud is a rare but very effective practice employed by traffickers who have an agent working for a telecommu-

---

[74] *Freeh Declaration, supra* note 24, ¶ 21.D.

[75] Interview with Manuel Estrella, *supra* note 42. When monitoring wire intercepts of telephones, Mr. Estrella occasionally hears one party inform the other one that he will send him an instant message with other information. *Id.*

[76] *Cellular Telephone Fraud Hearing, supra* note 30. Counterfeit fraud, also known as cellular phone piracy, includes cellular phone cloning, "tumbler-phone cloning," and "subscription fraud." *Id.*

[77] *Id.*

[78] *Id.* Criminal agents stake out "high-traffic areas, such as airports, bridges, tunnels or office complexes" and use the electronic scanners to obtain the Mobile Identification Number and Electronic Serial Number from private cellular calls. Then, software is used to program, or "clone," this information into the criminal's telecommunications instrument. *Id.*

[79] *Id.*

[80] *Id.*

[81] *Id.*

[82] *Id. at 13. See also Freeh Declaration, supra* note 24, ¶ 21.F for similar limitations on the scope of law enforcement.

nications carrier. This inside agent activates service for fraudulent users or cloned cellular phones.[83]

3. Negative Effects on Law Enforcement and the Telecommunications Industry

The damage to law enforcement efforts by such counterfeit telecommunications fraud practices is exponential. First, calls from a cloned phone are generally untraceable because drug trafficking agents use different pirated identification numbers for each call, stymieing law enforcement efforts as they obtain the required surveillance authorization, only to find that the agent has already changed to a new number.[84] Second, when traffickers pirate a consumer's cellular phone information, the charge for the calls, which are usually international, fall upon the consumer. The consumers then complain to their telecommunications company, who usually absorb the charges.[85] Thus, the telecommunications industry stands to save large amounts of money if it joins forces with United States law enforcement to shut down the abuse of the airwaves perpetrated by criminal networks and counterfeit fraud artists.

IV. ELECTRONIC SURVEILLANCE LEGISLATION

The wheels of electronic surveillance by law enforcement agencies were first set in motion by the Omnibus Crime Control and Safe Streets Act of 1968.[86] Title III of the Omnibus Act provided licensing grants as well as legislative limits for electronic surveillance for use in criminal investigations. Having considered the implications of freely-conducted surveillance with regard to individual rights, Congress carefully balanced the government's law enforcement with the protection of civil liberties. Aside from requiring probable cause under the Fourth Amendment, the Act requires that law enforcement may only utilize the interception of wire and oral communications by electronic surveillance in limited circumstances relating to criminal communications.[87] In addition, each application by law enforcement to intercept wire or oral communications must also be re-

---

[83] *Cellular Telephone Fraud Hearing*, *supra* note 30, at 13.

[84] *See generally Id.*

[85] *Id.* at 13.

[86] Pub. L. No. 90–351, 82 Stat. 197 (2000).

[87] § 2516, 82 Stat. at 211–14. Specifically, a Title III warrant based on probable cause may be issued to law enforcement only: (a) when other investigative techniques failed or appear to have failed, or are too dangerous to attempt; (b) for the investigation of serious, statutorily-specified felony offenses, and (c) for the interception of criminal communications. *Id.* § 2518.

viewed and authorized by a designated Department of Justice or state official before it may be presented for approval by a federal judge.[88]

A. Modernization of the Omnibus Act and Title III

In 1986, the Electronic Communications Privacy Act ("ECPA")[89] amended the Omnibus Act to incorporate modern innovations of advanced computer and telecommunications technologies.[90] The ECPA provides for electronic surveillance through "pen registers"[91] and "trap-and-trace" devices,[92] which identify the origin of wire or electronic communication directed to a facility under surveillance. Though these devices are much less intrusive than wiretaps and do not reveal the actual *contents* of any communication, they are effective when used by law enforcement to establish a link between parties to a criminal communication.[93] Congress preserved individual privacy rights by requiring that prior court approval be obtained before a pen register may be used to intercept electronic communications,[94] even though the Supreme Court held that use of pen registers does not qualify as a search.[95]

Section 2519 of the Omnibus Act requires reports to issue to the Administrative Office of the United States Courts concerning intercepted wire, oral, or electronic communications.[96] Every April, the director of that office is to submit "a full and complete report," called the "Wiretap Report,"

---

[88] § 2518, 82 Stat. at 218.

[89] Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510 (2000).

[90] *Yarbrough Declaration, supra* note 51, ¶¶ 3–4.

[91] 18 U.S.C. § 3124. A pen register is "'a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released. It does not overhear oral communications . . . .'" Smith v. Maryland, 442 U.S. 735, 735 n.1 (1979) (quoting United States v. N.Y. Tel. Co., 434 U.S. 159, 161 n.1 (1977)). A pen register is "'usually installed at a central telephone facility [and] records on a paper tape all numbers dialed from [the] line' to which it is attached." *Id.* at 735 n.1 (quoting United States v. Giordano, 416 U.S. 505, 549 n.1 (1974) (Powell, J., concurring in part and dissenting in part)).

[92] § 3124. "Trap-and-trace" devices provide information concerning the incoming call's origin and location. *Yarbrough Declaration, supra* note 51, ¶¶ 3–4.

[93] *Freeh Declaration, supra* note 24, ¶ 6. The information provided by these devices contributes to the evidence required for a Title III court order. *Id.*

[94] § 3121.

[95] *Smith*, 442 U.S. 745. The Court upheld as constitutional the warrantless installation of a pen register by police to record the numbers dialed from the telephone at the defendant's home. The Court concluded that installation of the device was not a Fourth Amendment search and, therefore, no warrant was required. *Id. But cf.* Katz v. United States, 389 U.S. 347 (1967) (holding that the electronic *listening and recording* device attached to outside of a public telephone by federal law enforcement agents constitutes a search and requires a warrant).

[96] Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90–351, § 2519, 82 Stat. 197, 222.

to Congress regarding the numbers of intercepts and includes detailed descriptions of each intercept.[97] In addition, the Wiretap Report features a variety of tables and charts diagramming the description, nature, frequency, and costs of the intercepts.[98]

1. The 2005 Wiretap Report

Examination of the most recent 2005 Wiretap Report reveals the extent to which law enforcement has utilized telecommunications and electronics to infiltrate drug trafficking and the illegal narcotics trade. "Portable devices" are the overwhelming leader in court-authorized intercepts among telecommunications channels,[99] and "narcotics" tallies the most court-authorized intercepts in the division of major criminal offenses.[100] In the past decade there has been a remarkable increase in the number of intercepts of portable communications devices involved in narcotics investigations.[101] The 1694 orders authorizing intercepts in 2005 led to 4674 arrests and 776 convictions.[102]

B. The Communications Assistance for Law Enforcement Act

Following the 1984 breakup of AT&T and the ensuing digital revolution enabling telecommunications subscribers to manage their private services in unprecedented ways, law enforcement recognized that cooperation with the nation's telecommunications carriers was critical to the continued interception of call-identifying information.[103] Congress also intervened to support this cooperation, passing the Communications Assistance for Law

---

[97] *Id.*

[98] ADMIN. OFFICE OF THE U.S. COURTS: THE WIRETAP REPORT (2005), http://www.uscourts.gov/wiretap05/contents.html [hereinafter THE WIRETAP REPORT].

[99] *Id* at 15-17 tbl. 2. Portable communications devices constituted 1610 intercepts out of 1773 total authorized intercepts for 2005 at the state and local level. *Id.* Examples of other channels for which intercepts were also authorized include personal residences (fifty-seven intercepts) and businesses (twenty-one intercepts). *Id.*

[100] *Id.* at 18-20 tbl. 3. Narcotics constituted 1433 intercepts out of 1773 total authorized intercepts for 2005 from state and local levels. The next closest offense was racketeering with ninety-four total authorized intercepts. *Id.*

[101] *Id.* at 30 tbl. 7. Table 7 traces intercepts reported from 1995–2005. It shows the number of "portable device" intercepts, non-existent before 2000, originating at 719, and "personal residence" as the next closest with 244. The table also shows narcotics as the leading major offense specified and marks the gradual increase in intercepts in that area for the past ten years. *Id.*

[102] *Id.* at 27-29 tbl. 6. Such positive results not only validate law enforcement's growing reliance on wire intercepts, but they also seem to justify the average cost of a court-authorized intercept order: $55,530. *Id.* at 24-26 tbl. 5. See *supra* text accompanying notes 48–50 for a discussion of the critical relationship between electronic surveillance and the investigation and prosecution of organized crime operations.

[103] *Yarbrough Declaration, supra* note 51, ¶¶ 5, 8, 9, 11.

Enforcement Act of 1994 ("CALEA")[104] to foil the use of the nation's telecommunications systems by organized crime networks. This Act uniformly addressed the nation's telecommunications carriers,[105] requiring them to design or modify their systems to meet specific assistance capability requirements that would ensure easy execution of court-ordered surveillance.[106] CALEA requires that carriers use up-to-date equipment, and that manufacturers of telecommunications equipment make CALEA-compliant modifications and updates available to the carriers.[107] Adopting a customary standard unique to the telecommunications industry, CALEA also calls for compliance with "publicly available technical requirements."[108] CALEA solicits the Federal Communications Commission ("Commission") to identify such publicly available standards, and to clarify compliance and capability requirements where the plain language of the legislation is deliberately general to allow for flexibility and interpretation.[109]

---

[104] Communications Assistance for Law Enforcement Act, Pub. L. 103–414, 108 Stat. 4279 (2000).

[105] § 102. CALEA defines "telecommunications carrier" as "a person or entity engaged in the transmission or switching of wire or electronic communications as a common carrier for hire." *Id.*

[106] § 103(a). This section sets forth the capability requirements with which telecommunications carriers must comply to support law enforcement in court-ordered electronic surveillance. Carriers have the responsibility to ensure that their networks are capable of: (1) "expeditiously isolating . . . all wire and electronic communications transmitted by the carrier within a service area," (2) "expeditiously isolating" call-identifying information of a target (origin, direction, destination, and termination of a call) that is reasonably available to the carrier; (3) providing such intercepted communications and call-identifying information to law enforcement; and (4) carrying out intercepts so that targets are not made aware of electronic surveillance by the government. *Id.*

[107] § 106. The Federal Bureau of Investigation and Department of Justice have worked to facilitate this process and lessen the costs for implementation by telecommunications carriers. In January 2000, for example, the FBI established a Flexible Deployment Program designed to facilitate CALEA compliance among telecommunications carriers. The FBI reviews information from the carrier in order to determine whether it will support the carrier's petition for a compliance extension filed with the Commission. *In re* The Communications Assistance for Law Enforcement Act, Section 107(c) Extension of Capability Requirements, *Order*, 17 F.C.C.R. 3672, ¶ 5 (Feb. 28, 2002). Additionally, in 2000, the FBI and DOJ reached an agreement with Lucent technologies in which the telecommunications equipment supplier would issue software to telecommunications carriers to remove any technological impediments that prevent compliance with CALEA, making lawfully-authorized electronic surveillance more simple and cost effective. Press Release, Dep't of Justice, Dep't of Justice and FBI Reach CALEA Agreement with Lucent Technologies and Bell Atl. Network Servs. (Apr. 13, 2000), *available at* http://www.usdoj.gov/opa/pr/2000/April/202jmd.htm.

[108] § 107 (a)(2).

[109] § 107. If these publicly available industry standards fail to issue technical requirements or standards, or if an agency or individual petitions the Commission identifying deficient industry standards, the Commission is responsible for establishing technical standards. Communications Assistance for Law Enforcement Act, 67 Fed. Reg. 21,999 (May 2, 2002) (codified at 47 C.F.R. pts. 22, 24, 64). Section 102 of CALEA delegates to the Commission the authority to establish findings which identify telecommunications carriers who

1. Who Must Comply? The Role of the Commission

A review of the services and carriers which the Commission determined to be subject to CALEA reveals the Commission's pivotal role in the law enforcement goal of efficient electronic surveillance. In August of 1999, the Commission designated six items from the DOJ and FBI "punch-list" subject to CALEA compliance.[110] One of these punch-list items, "dialed digit extraction," provides to law enforcement the digits dialed after the initial connection in pre-paid phone card services, when the user is prompted by the second carrier.[111] Also on the list is "subject-initiated dialing and signaling," which provides law enforcement with access to call forwarding and other features that enable users to reroute calls outside of a single loop.[112] The Commission further required compliance regarding "in-band and out-of-band signaling," which provides law enforcement with information regarding network signals and voice and text messages that criminals use to correspond.[113] Finally, the Commission adopted capability requirements for conference calling, such as "subject-initiated conference calls"[114] and instances of "party hold/join/drop."[115]

---

must comply with CALEA. 47 U.S.C. § 1001 (2000). Section 105 requires the Commission to establish regulations of security and integrity regarding the acquisition of a wire intercept. *Id.* § 1004.

[110] *In re* Communications Assistance for Law Enforcement Act, *Third Report and Order*, 14 F.C.C.R. 16794 (Aug. 26, 1999), *aff'd*, *In re* Communications Assistance for Law Enforcement Act, *Order on Remand*, 17 F.C.C.R. 6896 (Apr. 5, 2002) [hereinafter *Third Report and Order*]. The punch list features electronic surveillance capabilities that the FBI and DOJ requested the Commission consider in regard to CALEA compliance in order for electronic surveillance to keep pace with changes in telecommunications. *Id.* The *Third Report and Order* withstood challenge on remand, and was codified. *See* Communications Assistance for Law Enforcement Act, 67 Fed. Reg. 21,999 (May 2, 2002) (codified at 47 C.F.R. pts. 22, 24, 64).

[111] *Third Report and Order*, *supra* note 110, ¶ 112. Also referred to as "post cut-through digits," this procedure is most commonly found in the use of calling cards, when the caller dials an 800 number and follows prompts to dial a destination number. *Id.* Since the switch-over from AT&T analog to digital telecommunications, the destination number dialed had not been available for intercept by law enforcement. *See* discussion *supra* note 68.

[112] *Third Report and Order*, *supra* note 110, ¶ 76. Call forwarding is a feature that permits users to redirect calls, so that communications transmitted to that line may be transmitted to a different physical location and through a different wire loop. This practice was previously immune to electronic surveillance by law enforcement. *Yarbrough Declaration*, *supra* note 51, ¶ 10.

[113] *Third Report and Order*, *supra* note 110, ¶ 83. This requirement allows notification to be sent to the law enforcement agency whenever any "network message," such as a busy signal, call waiting signal, voicemail or text message notification, is sent to or from the subject under electronic surveillance. *Id. See supra* text accompanying note 74.

[114] *Third Report and Order, supra note 110,* ¶ 58. The adoption of this element of the punch list allowed law enforcement to monitor conversation content of all parties to a conference call, including parties placed on hold and parties dropped entirely from the conference call. *Id.*

More recently, the Commission's role has been to ensure that CALEA adapts to encompass emerging innovations in the telecommunications industry. In 2004, the Commission began requiring the CALEA-compliance of commercial mobile radio and wireless "push-to-talk" services[116] like Nextel and Verizon.[117] Most recently, the Commission expanded CALEA authority to include broadband Internet providers and "broadband telephony,"[118] the transmission or switching of voice communications using the broadband medium, more commonly known as interconnected Voice over Internet Protocol ("VoIP").[119] Prior to 2006, the Commission expressed concern that a requirement that all broadband Internet services comply with CALEA would fail to satisfy the three public interest factors.[120] But, in its most recent CALEA order, the Commission determined that these broadband Internet services should be subject to CALEA because they qualify as telecommunications carriers[121] under the two-pronged Substantial Replacement Provision ("SRP").[122] Specifically, the Commission con-

---

[115] *Id.* ¶ 68. This capability identifies all parties to a conversation at all times, and sends notification when a party is placed on hold, is released or disconnected from the call, or is reactivated from hold status. *Id. See discussion supra* note 73 regarding law enforcement's great need to identify the parties in a criminal conference call.

[116] Communications Assistance for Law Enforcement Act, 67 Fed. Reg. 21,999 (May 2, 2002) (to be codified at 47 C.F.R. pt. 64).

[117] *See supra* note 67 and accompanying text.

[118] *In re* Communications Assistance for Law Enforcement Act and Broadband Access and Services, *Notice of Proposed Rulemaking and Declaratory Ruling*, 19 F.C.C.R. 15676, ¶ 35 (Aug. 4, 2004) [hereinafter *CALEA NPRM*]. The Commission defines broadband as "those services having the capability to report . . . speeds in excess of 200 kilobits per second in the last mile." *Id. ¶ 35* According to the Commission, cable modem, satellite, and wireless are all forms of broadband Internet access providers. *Id.* ¶ 37.

[119] Due to its speed, convenience, and efficiency, VoIP is predicted to replace today's basic set up of local exchange services. Press Release, U.S. Dep't of Justice, with the FBI and DEA File Petition for Expedited Rulemaking with the FCC Requesting Resolution to Issues Surrounding the Implementation of the Communications Assistance for Law Enforcement Act (CALEA) (Jan. 28, 2004). The Commission recently decreed that broadband Internet access providers and VoIP services are given until May 14, 2007 to become CALEA compliant, and must submit periodic reports to the Commission to ensure that they will meet the deadline. *In re* Communications Assistance for Law Enforcement Act and Broadband Access and Services, *Second Report and Order and Memorandum Opinion and Order*, 21 F.C.C.R. 5360, ¶¶ 1, 8 (May 12, 2006) [hereinafter *Second Report and Order*] ("[A]ll carriers providing facilities-based broadband Internet access and interconnected VoIP services must be in compliance with section 103 of CALEA by May 14, 2007."). *See also* Am. Council on Educ. v. FCC, 451 F.3d 226 (D.C. Cir. 2006) (aff'd the order which requires VoIP and broadband Internet services to be CALEA compliant).

[120] *See infra* text accompanying note 127. The Commission argued that requiring compliance in "underserved" areas would negatively impact the protection of competition and the development of new technologies. *CALEA NPRM, supra* note 118, ¶ 49.

[121] Communications Assistance for Law Enforcement Act, Pub. L. No. 103–414, § 102, 108 Stat. 4279, 4280 (1994).

[122] § 102(8)(b)(ii) (The Substantial Replacement Provision provides the Commission with a test to determine whether a service provider qualifies as a telecommunications carrier

cluded that broadband Internet provision satisfies the first prong of the SRP because it replaces a substantial proportion of the local telephone exchange service used for dial-up Internet service.[123] The Commission also concluded that VoIP services satisfy the second prong of the SRP, which classifies any service as a telecommunications carrier and thus subject to CALEA whenever such classification furthers the public interest.[124] Because it is in the public interest to assist law enforcement in its ability to lawfully conduct electronic surveillance in the face of a rapidly progressing telecommunications industry, the Commission classified VoIP as telecommunications subject to CALEA.[125]

2. *The Effective Balance Integrated in CALEA*

CALEA is particularly effective because of the elements of reasonableness imported from its statutory predecessor, the Omnibus Act. Similar to the Omnibus Act regulation, CALEA only permits electronic surveillance assistance from telecommunications providers pursuant to a court order.[126] In addition, the statutory directive for the Commission's implementation of CALEA is composed of three public interest factors: promoting fair competition, encouraging the development of new technologies, and protecting public safety and national security.[127] Thus, CALEA balances the business endeavors of telecommunications carriers with those of law enforcement by prohibiting law enforcement agencies from impeding any innovative development or manufacture of equipment features.[128] Furthermore, directing the Commission to determine whether compliance would be problematic for a carrier, CALEA instructs the Commission to consider "cost-effective methods" of capability assistance[129] and United States policy toward industry: to stimulate innovation and technology.[130] Consistent with this policy, telecommunications carriers are only required to turn over call-

---

subject to CALEA. The service is a telecommunications carrier, under the first prong of the test, if it "is a replacement for a substantial portion of the local telephone exchange service," and under the second prong of the test, if "it is in the public interest to deem such a person or entity to be a telecommunications carrier . . . ." *Id.*

[123] *CALEA NPRM, supra* note 118, ¶ 37.

[124] *Id.*

[125] *Id.*

[126] § 105. See also *supra* notes 87–88 and accompanying text for discussion of Title III of Omnibus Act.

[127] *CALEA NPRM, supra* note 118, ¶ 49.

[128] § 103.

[129] § 109. This determination is made after the Commission weighs the financial resources of the telecommunications carrier and the effect that compliance will have on the carrier's competition. *Id.*

[130] § 109(b)(1)(G) (dictating that aside from considering burdens on the carriers imposed by compliance, the Commission is encouraged to facilitate new and public technological innovation).

identifying information when it is "reasonably available" to the provider,[131] and then only after "a reasonable time and conditions" specified by the court.[132] Finally, CALEA authorizes the Attorney General to pay telecommunications carriers for all reasonable costs accrued in direct association with compliance measures.[133]

3. CALEA's Pursuit of Flexibility Leaves Room for Minor Guideline Modifications

Despite the constructive elements, the current CALEA framework suffers from shortcomings that may leave law enforcement powerless to detect certain kinds of criminal communications. First, the statute's reasonable balance and flexibility standard does not enable the Commission to guarantee full and swift compliance. Under the "safe harbor" provision of CALEA, a telecommunications carrier attempting to comply with the capability requirements may petition the Commission for unlimited two-year extensions of the compliance deadline.[134] Thus, while the eighteen month timetable the Commission established for VoIP providers in August of 2005 may seem reasonable to allow providers time to achieve compliance, criminal groups can continue to exploit the services of Internet voice communications providers who petition for multiple extensions. Perhaps in recognition of this loophole, the Commission recently declared that *all* carriers are obliged to become CALEA-compliant, and established a fixed timetable for compliance of broadband providers subject to CALEA by May 14, 2007,[135] while significantly restricting the safe harbor provisions available to all other carriers.[136]

But some flaws in their implementation of CALEA remain problematic. In particular, the Commission has not yet enforced CALEA compliance with regard to computer instant messaging services. These services are becoming a popular channel through which drug traffickers may coordinate illicit action quickly and undetected.[137] Furthermore, subjecting this method of communication to CALEA compliance would likely pass the two-pronged Substantial Replacement Provision test under the statute.[138] The first prong is satisfied because instant messaging is an electronic

---

[131] § 103.

[132] § 108.

[133] § 109. This provision was included because legislators recognized that "some existing equipment, services or features will have to be retrofitted" and costs will be incurred when telecommunications providers modify "existing equipment, services or features to comply with the capability requirements." H.R. REP. NO. 103-827, pt. 1, at 12 (1994).

[134] § 107.

[135] *Second Report and Order, supra* note 119, ¶¶ 1, 8.

[136] *Id.* ¶¶ 27-37.

[137] *See supra* note 75 and accompanying text.

[138] § 102. *See discussion supra* note 122.

communications service that, because it is speedy and inexpensive, may constitute at least a temporary replacement for a portion of the local telephone exchange service for many people. The second prong of the provision is also fulfilled because it would likely be in the public interest to classify this service as a telecommunications service for law enforcement purposes. Although the Commission appears to be taking a more proactive approach, as indicated in their recent restrictions on compliance safe harbors, the pervasive use of technological innovations in communications by organized crime operators requires that the Commission continue to expand the reach of CALEA to allow effective law enforcement interdiction.

V. ELECTRONIC SURVEILLANCE IN THE BALANCE OF INDIVIDUAL RIGHTS

Expanding electronic surveillance to virtually all popular cellular phone and Internet channels of communications under CALEA is a natural and necessary progression considering both the drug smuggling activities coordinated over those telecommunications lines, as well as the devastating impact of narcotics infiltration on American society. Nevertheless, it is difficult to ignore the fact that the campaign for stricter compliance with CALEA could compromise individual privacy rights for average, law-abiding Americans.[139] Regardless of the positive impact that electronic surveillance pursuant to CALEA has on inner cities and communities as a whole, it is likely that many individuals would strongly object to the possible release of personal information to law enforcement. Although Title III prohibits surveillance of non-criminal communications,[140] it is problematic that there is no public accountability to ensure that private, non-criminal communications remain private. In assessing these public interest and privacy concerns, it is worth considering them in the context of the War on Terror[141] and the controversial steps taken by the current administration to combat terrorism.

---

[139] This sentiment has been noted by the FCC: "An approach like the one we adopt today is not without legal risk." *In re* Communications Assistance for Law Enforcement Act and Broadband Access and Services, *First Report and Order and Further Notice of Proposed Rulemaking*, 20 F.C.C.R. 14,989, 15,041 (Sept. 23, 2005) (Statement of Comm'r Kathleen Q. Abernathy), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-153A3.pdf. ("An approach like the one we adopt today is not without legal risk.").

[140] 18 U.S.C. § 2511 (2000). *See also* sources cited *supra* note 87 and accompanying text.

[141] President George W. Bush, Address to a Joint Session of Congress and the American People (Sept. 20, 2001), *available at* http://www.whitehouse.gov/news/releases/2001/09/20010920-8.html [hereinafter President Bush Sept. 20, 2001 Address]. The modern war against terrorism was born on Sept. 11, 2001, when terrorists hijacked planes and used them as weapons to attack New York City and Washington, D.C. See Dan Balz & Bob Woodward, *America's Chaotic Road to War: Bush's Global Strategy Began to Take Shape in First Frantic Hours After Attack*, WASH.

A. Organized Crime Today: "New Mafia" Trafficking Meets Worldwide Terrorism

1. Organization and Infrastructure

The fight against drug trafficking and organized crime draws many parallels to the War on Terror in which this country has been engaged since 2001.[142] Just as drug traffickers became "the new Mafia" at the end of the twentieth century,[143] terrorist organizations have carved out a unique niche in the vast landscape of organized crime in the twenty-first century.[144] The harm to the United States from drug trafficking is inflicted by an enemy kingpin at a location outside of the United States. The kingpin employs cells in countries around the world to carry out his goals, which are accomplished by preying on the weaknesses of American citizens and jeopardizing their safety.[145] Similarly, a terrorist organization may consist of hundreds of individuals operating worldwide, who carry out the missions coordinated by the leader.[146] The Medellín cartel was able to secure and

---

POST, Jan. 27, 2002, at A01. President George W. Bush was informed of the attack on the World Trade Center while reading to a class of second-grade children in Sarasota, Florida. He later described his thoughts upon hearing the news of the attack: "They had declared war on us, and I made up my mind at that moment that we were going to war." *Id.* In a televised address from the Oval Office the night of Sept. 11, the President's first televised broadcast regarding "the war against terrorism," he stated to the American public: "I've directed . . . our intelligence and law enforcement communities to find those responsible and to bring [the perpetrators] to justice. We will make no distinction between the terrorists who committed these acts and those who harbor them." President George W. Bush, Statement by the President in his Address to the Nation (Sept. 11, 2001), *available at* http://www.whitehouse.gov/news/releases/2001/09/20010911-16.html. The perpetrators were identified and revealed to America as a collection of terrorist organizations called Al Qaeda. President George W. Bush, Address to a Joint Session of Congress and the American People (Sept. 20, 2001).

[142] *See* sources cited *supra* note 141.

[143] *See* discussion *supra* Part II.A..

[144] President Bush underscored this notion: "Al Qaeda is to terror what the Mafia is to crime. But its goal is not making money; its goal is remaking the world—and imposing its radical beliefs on people everywhere." President Bush Sept. 20, 2001 Address.

[145] Grayson, *supra* note 34, at 147.

[146] *See* Balz & Woodward, *supra* note 141, at A01. The Islamic Jihad movement employs thousands of terrorists in more than sixty countries. President Bush Sept. 20 Address, *supra* note 141. For example, Al Qaeda is based out of Afghanistan, but its missions are transmitted to its soldiers worldwide. Specifically, Al Qaeda employs fighters and trainers throughout Afghanistan, Bosnia, Chechnya, Somalia, Sudan, the Philippines, Egypt, and Libya among other nations. PROFILE, DEPARTMENT OF STATE (1997), *reprinted in* AMERICA CONFRONTS TERRORISM 172 (John Prados ed., 2002) [hereinafter PROFILE]. Likewise, the Medellín and Cali drug cartels were headed by kingpins in Colombia, with smugglers and various agents carrying out functions internationally. Whereas the Cali kingpins orchestrated the smuggling of narcotics covertly, Al Qaeda's very public operations, including frequent broadcasts of its extremist goals and missions in speeches delivered through the mass media on videotape, are reminiscent of the Medellín cartel's public demonstrations of

maintain power in the 1980s because of its willingness to overtly employ terrorism techniques to remove threats of extradition, and to force the Colombian government to withdraw implementation of its drug policy.[147] The decline of the Medellín during the early 1990s was due in part to the rise of the rival Cali cartel, which also benefited from terrorist techniques, specifically with regard to structural communication.[148]

2. Debilitating Effects of Organized Crime on Government Efficiency and the American People

Terrorism threatens American security and freedom in a way that is closely mirrored by the formidable threat to the health and well-being of American citizens brought on by the ills of drug proliferation and smuggling. The far-reaching impact of drugs and organized crime fashioned drug trafficking into a "legitimate national security issue."[149] Today, terrorism is a predominant concern of the American public, perhaps the biggest threat to national security, and it represents one of the highest priority issues for the current Administration.[150] Not unlike the War on Drugs, threats

---

violence and power. *Frontline: Drug Wars Television Broadcast Transcript, supra* note 8. In August 1996, Al Qaeda founder and terrorist mastermind Osama bin Laden issued statements to the press detailing the group's goals, which included liberating Muslim holy sites and supporting Islamic militant groups around the world. PROFILE, *supra* note 146, at 172. In the wake of the September 11 attacks, bin Laden publicly threatened further harm against the United States and the West. John Prados, *Osama bin Laden, in* AMERICA CONFRONTS TERRORISM 161, 167 (John Prados ed., 2002). On October 7, 2001, bin Laden stated that a group of Muslim extremists was blessed with the responsibility "to destroy America," and called on every Muslim to "rise and defend his religion." OSAMA BIN LADEN, BIN LADEN STATEMENT, OCT. 7, 2001: "THE SWORD FELL" (2001), *reprinted in* AMERICA CONFRONTS TERRORISM 12–13 (John Prados ed., 2002).

[147] *Frontline: Drug Wars Television Broadcast Transcript, supra* note 8. From the mid- to late-1980s, Medellín guerillas threatened and killed proponents of extradition, including Colombian national justice ministers, politicians, law enforcement officials, and journalists. The cartel also financed random public bombings that deteriorated public morale and imposed a culture of death and destruction on Colombian citizens. *Id.*

[148] *Drug Wars: Colombian Traffickers, supra* note 14. The Cali cartel was a model of efficiency because of its use of terrorist group techniques. For example, Cali separated its many workers into units or cells who received orders on a primarily individual and covert basis, with each cell knowing very little about the other employees and their duties. *Id.*

[149] KELLY, *supra* note 1, at 100. See *supra* note 33 for a discussion of the priority given to the War on Drugs as a domestic policy issue.

[150] Terrorism has become the top priority issue for the DOJ. *See* RICHARD A. CLARKE, AGAINST ALL ENEMIES: INSIDE AMERICA'S WAR ON TERROR 256 (2004). Prior to Sept. 11, as the perceived threat to national security from terrorism was not great, there was no significant counterterrorism spending. *Id.* This was complemented and perhaps fostered by limited public knowledge of global terrorism, and low public interest regarding counterterrorism programs. John Prados, *Introduction, in* AMERICA CONFRONTS TERRORISM, *supra* note 146, at 3. The attacks of September 11 made the terrorism issue personal to Americans, and thus the war on terrorism became supported by public demand. *Id.* at 4.

from terrorist organizations all over the globe command a significant amount of United States government resources in the War on Terror.[151]

3. Government Responses and the Public's Reaction to the Threats

The similarities between the War on Drugs and the War on Terror are further evident in the broadening of executive power and redefinition of civil liberties in the name of national security. The War on Drugs spawned narcotics regulations which served as a justification for increasing surveillance on American citizens, particularly members of minority groups.[152] Likewise, as a direct reaction to the terrorist attacks of September 11, 2001, United States government and law enforcement officials employed procedures like racial profiling of Arab and Muslim Americans in the War on Terror.[153] On September 23, 2001, President Bush issued an Executive Order on Terrorist Financing, naming twenty-seven groups and individuals, all Arab or Muslim, as having terrorist links.[154] Perhaps as an outgrowth of this treatment by United States government forces toward Arab and Muslim individuals, there is evidence that much of the American public also became hostile toward fellow citizens who were Arab or Muslim.[155]

---

[151] President Bush Sept. 20, 2001 Address, *supra* note 141. The President stated: "Our war on terror begins with al Qaeda, but it does not end there. It will not end until every terrorist group of global reach has been found, stopped and defeated." *Id.* During that address, President Bush announced the creation of a Cabinet-level position in the Office of Homeland Security, appointing military veteran Tom Ridge as Secretary of Homeland Security and deeming that office responsible for orchestrating a national strategy for combating terrorism. *Id.* See *supra* note 33 for a discussion of the similar appointment of retired military veterans to positions of czar in the War on Drugs. Whereas all national security spending totaled $9 billion in 1995, homeland security spending by 2002 reached $29.3 billion, $9.8 billion of which was a result of a supplemental appropriation following September 11. MICHAEL E. O'HANLON ET AL., PROTECTING THE AMERICAN HOMELAND: ONE YEAR ON 137 (2002).

[152] Grayson, *supra* note 34, at 157. This includes more frequent invasions of privacy through electronic surveillance and police searches. *Id.*

[153] AS'AD ABUKHALIL, BIN LADEN, ISLAM, AND AMERICA'S NEW "WAR ON TERRORISM" 85–86 (2002). In the aftermath of the attacks, the arrests of Arabs and Muslims exceeded 1200. Only one of these arrests connected a suspect with the hijackers. *Id.*

[154] Exec. Order No. 13,224, 66 Fed. Reg. 49,079 (Sept. 25, 2001). The Order not only blocked transactions and property interests of these groups and individuals, but expanded the class of targeted groups to include all those "associated with" designated terrorist groups; it also reserved the ability to block assets and deny access to United States markets to any banks or worldwide organization which does not freeze terrorist assets. *Id.*

[155] ABUKHALIL, *supra* note 153, at 91. Unrest was evident on commercial airlines following the attacks; there are several reports of pilots and passengers acting in strong opposition to allowing Arab looking men to board planes. *Id.* at 82.

B. Differences Between Legislative Responses to the War on Drugs and the War on Terror

The power wielded by the United States government in increasing surveillance of citizens following September 11 has been met with considerable opposition. Signed into law on October 26, 2001, the USA PATRIOT Act ("Patriot Act")[156] expanded the authority of United States law enforcement in fighting terrorist acts in the United States and abroad, and increased intelligence authority across telecommunications channels.[157] Aptly named, the Act was drafted with the intention of ensuring the trust of American citizens in the United States government at a time when the people were frightened and needed protection.[158] However, implementation of the Patriot Act has created a popular backlash against the measures taken by the Administration.[159] CALEA, which can be viewed as the Patriot Act's legal counterpart in the War on Drugs, has not met with much opposition from the American public.

1. Government Responses to Exigencies Created by Terrorism Trigger Incendiary Reactions

An apparent reason for such incongruity in public response may be that while the Patriot Act was rather hurriedly enacted as an immediate response to the attacks on the World Trade Center, CALEA was a piece of legislation that had the benefit of deliberative debate and drafting. Accordingly, an extensive legislative history precedes CALEA, exhibiting considerable discussion and a balancing of legislative goals.[160] Yet, CALEA is

---

[156] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107–56, 115 Stat. 272 (2001).

[157] O'HANLON ET AL., *supra* note 149, at 128. Detractors of the Patriot Act have derided it for infringing upon individual and civil rights in its amendments to the Foreign Intelligence Surveillance Act of 1978 and the Electronic Communications Privacy Act of 1986 which expands federal powers to intercept and share private telecommunications information. *Id.*

[158] CLARKE, *supra* note 150, at 257.

[159] *Id.* at 256–57. For example, the Attorney General's attempted surveillance increases included authorizing the FBI to monitor library reading records for the possibility of terrorist or fundamentalist literature falling into the wrong hands. *See id.* at 257. Instead of increasing the public's trust in the government, allowing for such actions without judicial review may have instead served to "fundamentally shake the confidence" of Americans in the government's capacity to safeguard civil liberties while defeating the terrorists. *Id.*

[160] H.R. REP. NO. 103-827, pt. 1. CALEA's drafters sought to "preserve the balance" reflected in the Omnibus Act and the ECPA. *Id.* at 14–15. According to CALEA's legislative history, the bill sought to balance the following core principles: "(1) to preserve a narrowly focused capability for law enforcement agencies to carry out properly authorized intercepts; (2) to protect privacy in the face of increasingly powerful and personally revealing technologies; and (3) to avoid impeding the development of new communications services and technologies." *Id.* at 15. Regarding privacy issues affected by court-ordered wire-

also a complicated piece of legislation, involving significant technical terminology to the extent that it may not sustain the interest or consideration of the average American citizen or command significant media attention. Nevertheless, the complicated language and subject matter is not a pretense for permitting law enforcement to exploit the ignorance of the American public by infringing on individual privacy rights. The subject of encroachment on individual rights has become more widely scrutinized and publicized in gauging the effectiveness of the responses to the War on Terror.

2. Objection to Non-Legislative Responses by Government to the War on Terror

Recently, a program of domestic surveillance on American citizens came crashing to the foreground in the War on Terror, allowing CALEA and the surveillance measures used in the War on Drugs to truly shine by contrast. On December 16, 2005, The New York Times revealed that, shortly after September 11, 2001, President George W. Bush personally authorized the National Security Agency ("NSA") to eavesdrop on telephone and e-mail communications between individuals in the United States and overseas without first obtaining a warrant.[161] The Office of the Attorney General justified this practice, stating that intercepting communications of those who may be linked to terrorists is "clearly reasonable" under the Fourth Amendment.[162] Using balancing approach terminology, the Attorney General declared that the interest of the NSA in defending the nation is "the most compelling interest possible," and outweighs any individual privacy interests at stake.[163]

Despite the fact that law enforcement practices under CALEA and the Omnibus Act have previously and rather proficiently enlisted major telecommunications carriers for assistance in conducting electronic surveillance of private lines, news of domestic spying by the NSA has stirred up a considerable amount of dissension among the American citizenry, as well as among politicians.[164] As is the case with CALEA, NSA surveillance

taps under CALEA, legislators noted: "[A]s the potential intrusiveness of technology increases, it is necessary to ensure that government surveillance authority is clearly defined and appropriately limited." *Id.* at 18.

[161] James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1. This domestic spying was initiated in response to the terrorist attacks of Sept. 11, 2001.

[162] Letter from Asst. Att'y Gen. William E. Moschella to Sen. Pat Roberts, et al., 4 (Dec. 22, 2005).

[163] *Id.*

[164] Dan Eggen & Walter Pincus, *Varied Rationales Muddle Issue of NSA Eavesdropping*, WASH. POST, Jan. 27, 2006, at A05. A parallel can be drawn between the public effects of the current Administration's use of the NSA and the Nixon Administration's use of the DEA to further political objectives. Following its inception, the DEA faced criticism for being overzealous in its drug enforcement tactics, specifically with regard to potential

depends upon cooperation from major telecommunications carriers to assist in intercepting conversations of persons who arouse suspicion because of their alleged ties to a criminal organization. The most apparent reason for the discrepancy in public reception of the practices is that CALEA and the Omnibus Act are codified pieces of legislation that must satisfy high standards required for obtaining court-ordered intercepts pursuant to statute,[165] whereas the NSA domestic surveillance was authorized not by enacted legislation but by covert order from the President. Moreover, the NSA's standard for conducting an intercept is merely a "reasonable basis to believe" a target is linked to Al Qaeda or an affiliated terrorist organization.[166]

In commencing his program of domestic spying, Bush never sought Congressional approval, relying instead on an asserted "constitutional power granted to presidents, as well as . . . a statutory power."[167] Despite such strong claims of authority, the President did not confidently wield this power, but rather exerted it by secret order.[168] The outrage over this clandestine operation which appears to jeopardize civil liberties is fueled by the public's uncertainty regarding the extent to which they were misled into compromising individual rights.[169] CALEA and the Omnibus Act, on the other hand, benefit from clearly-defined and publicly available guidelines and constraints, supported by both the Fourth Amendment and Congressional intent. The notion of reasonableness is considerably more evident with regard to the practice of electronic surveillance under CALEA and the Omnibus Act.[170] Finally, the balance inherent in CALEA's goals of promoting fair competition, encouraging innovation, and protecting public safety and national security,[171] provides for unique cooperation between law enforcement and business as working pursuant to mutual agreement, not an order from the President.[172]

Fourth Amendment violations occurring during searches and seizures of homes and wiretaps. *Frontline: Drug Wars Television Broadcast Transcript*, *supra* note 8.

[165] *See supra* note 122 and accompanying text.

[166] Eggen & Pincus, *supra* note 164.

[167] *Id.* Attorney General Alberto Gonzales said the Bush administration did not seek legislation after determining it would be virtually impossible to obtain. *Id.*

[168] *Id.* White House spokesman Scott McClellan said that the Administration feared exposure of the classified program. In truth, the briefings Bush gave about the program were "limited to the 'Gang of Eight': the speaker and minority leader of the House; the majority and minority leaders of the Senate; and the chairmen and ranking Democrats on the two intelligence committees." This group was not permitted to take notes or discuss the briefing within their offices or with their fellow members of Congress. *Id.*

[169] *Id.*

[170] 47 U.S.C. § 1008 (2000). Reasonableness is embodied in CALEA provisions requiring cost-effective methods of capability assistance and compliance. *Id. See* discussion *supra* Part IV.B.2.

[171] *CALEA NPRM*, *supra* note 118, ¶ 49.

[172] *See* discussion *supra* note 107 for an example of the cooperative efforts between law enforcement and industry.

VI. CONCLUSION

While Italian crime syndicates once relied on muscle and lax government surveillance to subject the United States to their narcotics empire, today's drug trafficking organizations and modern mobsters were met with a War on Drugs and legislation aimed at intercepting their communications. In order to survive, South American and Mexican drug trafficking organizations invested vast resources in local drug manufacturing and technological advancements to coordinate smuggling operations through covert telecommunications. The constraints of Title III of the Omnibus Act made it difficult for law enforcement to monitor the cartels following the breakup of AT&T and the demise of analog services in favor of digital communications. Since Congress authorized telecommunications carriers to collaborate with law enforcement on electronic surveillance in CALEA, however, the drug traffickers have once again become locked in the crosshairs of effective law enforcement surveillance.

CALEA stands out for being effective without being controversial, despite the fact that it can be used for the interception of virtually any cellular or Internet communication. CALEA was carefully drafted to allow the telecommunications industry to innovate and flourish while simultaneously assisting law enforcement in halting criminal activities occurring over its communications lines. Moreover, CALEA succeeds in striking a balance between personal privacy and national security by updating Title III to adapt to modern telecommunications advancements without doing away with the probable cause requirement of the Fourth Amendment.[173] Still, some minor adjustments will need to be made in order to ensure CALEA does not fall behind in its electronic surveillance efficacy. The Commission must establish compliance benchmarks and begin enforcing extension periods, and must demand the utmost cooperation from carriers to conducting electronic surveillance on all versions of broadband, VoIP, and instant messaging services.

CALEA stands as a model of how proper electronic surveillance measures should operate. Thus, it stands in direct opposition to the domestic surveillance initiative to uncover potential terrorists, which was unilaterally authorized by the President with the disputed justification of constitutional war powers. The United States, through Congress and the Commission, should continue to expand the reach of CALEA to ensure that law enforcement can effectively fight organized criminal activity, including terrorism, while protecting civil liberties.

---

[173] 18 U.S.C. § 2510 (2000). In addition, Title III authorizes the interception of wire and oral communications by electronic surveillance only in very limited circumstances relating to criminal communications. *Id.*