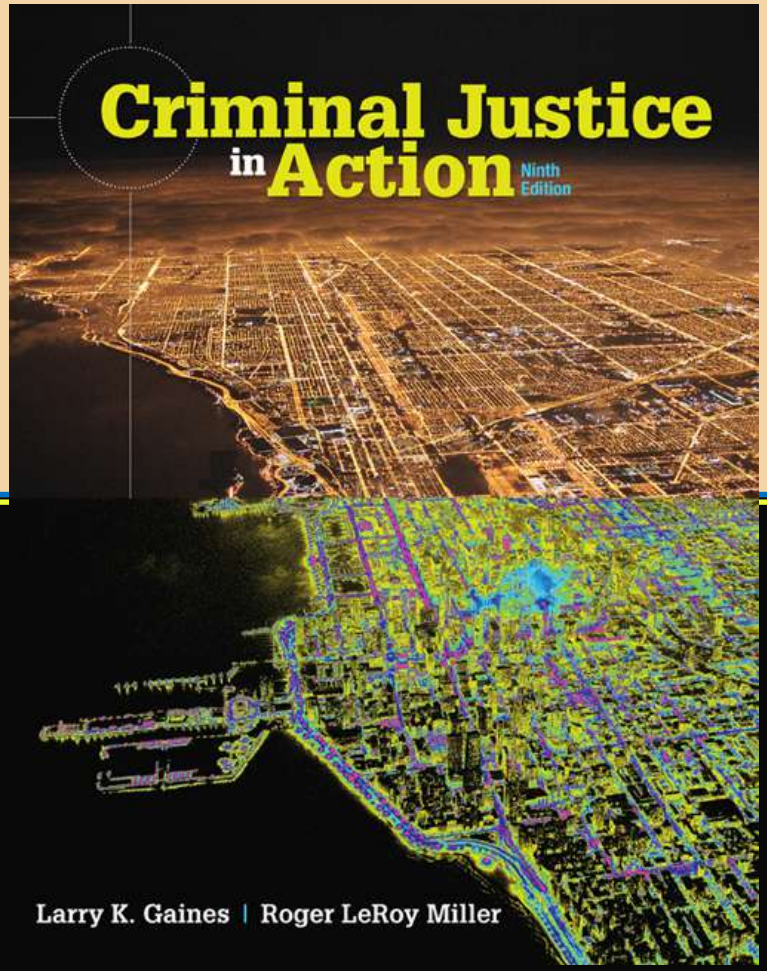

Chapter 16

Today's Challenges: Security vs. Liberty, Cyber Crime, and White-Collar Crime

Learning Objective 1

- Summarize the three federal laws that have been particularly influential on our nation's counterterrorism strategies.

Jewel Samad/AFP/Getty Images

Security vs. Liberty

- National security and privacy
  - Congress passed the Foreign Intelligence Surveillance Act (FISA) in 1978.
  - The Antiterrorism and Effective Death Penalty Act (AEDPA) hampers terrorist organizations by cutting off their funding.
  - The Patriot Act

Security vs. Liberty

- *Section 201:* Enables government agents to wiretap the communications of any persons suspected of terrorism or the dissemination of chemical weapons.
- *Section 204:* Makes it easier for government agents to get a warrant to search stored e-mail communications held by Internet Service Providers (ISPs).
- *Section 206:* The "roving wiretap" provision removes the requirement that government agents specify the particular places or things to be searched when obtaining warrants for surveillance of suspected terrorists.
- *Section 210:* Gives government agents enhanced authority to access the duration and timing of phone calls, along with phone numbers and credit cards used to pay for cell phone service.
- *Section 213:* The "sneak and peak" provision removes the requirement that government agents give notice to a target when they have searched her or his property."
- *Section 214:* Removes the requirement that government agents prove that the subject of a FISA search, discussed earlier in the section, is actually the "agent of a foreign power."
- *Section 215:* The "business records" provision permits government agents to access "business records, medical records, educational records and library records" without showing probable cause of wrongdoing if the investigation is related to terrorism activities.

Learning Objective 2

- Explain why private expectations are so important to the federal government's metadata surveillance operations.

Win McNamee/Getty Images

Security vs. Liberty

- Revelation that NSA had been monitoring cell phone and Internet activity of about 113 Americans without probable cause or a warrant from the FISA court
  - Government agents can search and seize, without a warrant, information voluntarily disclosed to third parties.
  - *Smith v. Maryland* (1979) held that a defendant had no expectation of privacy when he voluntarily turned over phone numbers to a third party.

Learning Objective 3

- Distinguish verbal threats that are protected by the Constitution from verbal threats that can be prosecuted as “true threats.”

Brian Kersey/Getty Images

Security vs. Liberty

- True threat law
  - In *Virginia v. Black* (2003), the Supreme Court held that the act of burning a cross was not enough to constitute a crime, and that the state must also prove that the act was done to place a specific victim "in fear of bodily harm or death."
- Finding and capturing "known wolves"

Learning Objective 4

- Outline the three major reasons why the Internet is conducive to the dissemination of child pornography.

P. C. Vey/The New Yorker Collection/Cartoonbank.com

Cyber Crime

- Cyber crime is any criminal activity occurring via a computer in the virtual community of the Internet.
- Child pornography
  - Speed
  - Security
  - Anonymity

Cyber Crime

- Cyberattack: attempt to damage or disrupt computer systems or electronic networks operated by computers
  - Infrastructure security

Cyber Crime

- Cyber fraud
  - Theft of personal information
- Cyber theft
  - Identity theft
  - Phishing

Cyber Crime

FIGURE 16.2 The Costs of Cyber Crime

After polling adults in twenty-four countries, including the United States, researchers associated with the American security software company Symantec estimated that more than 1.5 million computer users worldwide are victims of cyber crime each day. As the graph below shows, 83 percent of the financial costs associated with cyber crime are the result of fraud, theft, or computer repairs made necessary by the wrongdoing.

Source: *2012 Norton Report* (Mountain View, Calif.: Symantec, 2014), 8.

Cyber Crime

- Cyberstalking
  - Harassing a person through the Internet and putting that person in reasonable fear for his or her safety
- Cyberbullying
  - Willful and repeated emotional harm inflicted through electronic devices

Learning Objective 5

- Describe the three following forms of malware: a) botnets b) worms and (c) viruses.

Nathan Alliard/Getty Images

Cyber Crime

- Hacker
  - Person who breaks into another person's computer
- Malware
  - Any program that is harmful to a computer or computer user
- Botnets
  - Networks of computers that have been appropriated by hackers without the knowledge of their owners
- Worms
  - A program that is capable of reproducing itself as it spreads from one computer to the next
- Viruses
  - Able to reproduce itself, but must be attached to an infested host file in order to travel

Learning Objective 6

- Explain how the Internet has contributed to piracy of intellectual property.

Bloomberg via Getty

Cyber Crime

- Pirating intellectual property
  - Intellectual property is the products that result from intellectual, creative processes
  - Includes piracy of books, films, music, and software
  - An estimated 43% of all software is pirated

Cyber Crime

- Cyber forensics
  - Officers cannot put yellow tape around the computer screen or dust the Web site.
  - Digital evidence is stored or transmitted by an electronic device.
- Cyber sleuthing
  - Tools to bypass technology employed by cyber criminals
  - Jurisdictional challenges

Learning Objective 7

- Indicate some of the ways that white-collar crime is different from violent or property crime.

Embezzlement
Embezzlement is a form of employee fraud in which an individual uses his or her position within an organization to *embezzle*, or steal, the employer's funds, property, or other assets. Pilferage is a less serious form of employee fraud in which the individual steals items from the workplace.

Tax Evasion
Tax evasion occurs when taxpayers underreport (or do not report) their taxable income or otherwise purposely attempt to evade a tax liability.

Credit-Card and Check Fraud
Credit-card fraud involves obtaining credit-card numbers through a variety of schemes (such as stealing them from the Internet) and using the numbers for personal gain. Check fraud includes writing checks that are not covered by bank funds, forging checks, and stealing traveler's checks.

Mail and Wire Fraud
This umbrella term covers all schemes that involve the use of mail, radio, television, the Internet, or a telephone to intentionally deceive in a business environment.

Securities Fraud
Securities fraud covers illegal activity in the stock market. Stockbrokers who steal funds from their clients are guilty of securities fraud, as are those who engage in *insider trading*, which involves buying or selling securities on the basis of information that has not been made available to the public.

Bribery
Also known as *influence peddling*, bribery occurs in the business world when somebody within a company or government sells influence, power, or information to a person outside the company or government who can benefit. A county official, for example, could give a construction company a lucrative county contract to build a new jail. In return, the construction company would give some of the proceeds, known as a *kickback*, to the official.

Consumer Fraud
This term covers a wide variety of activities designed to defraud consumers, from selling counterfeit art to offering "free" items, such as electronic devices or vacations, that include a number of hidden charges.

Insurance Fraud
Insurance fraud involves making false claims in order to collect insurance payments. Faking an injury in order to receive payments from a workers' compensation program, for example, is a form of insurance fraud.

White-Collar Crime

- What is white-collar crime?
  - Covers a broad range of illegal acts involving "lying, cheating, or stealing"
  - Not an official category of criminal behavior
- Different techniques
  - Have legal access to the place the crime occurs
  - Are spatially separated from the victim
  - Behave in a manner that is superficially legitimate

White-Collar Crime

- Three main techniques of white-collar criminals to commit crime
  - Deception
  - Abuse of trust
  - Concealment and conspiracy
- Victims of white-collar crime:
  - Sometimes the victims are obvious; in other instances however, they are a little more difficult to define.
  - Can be one person, multiple people, society, or the environment

Learning Objective 8

- Explain the concept of corporate violence.

Corporate Violence

- Corporate violence
  - Physical harm to individuals or the environment that occurs as the result of corporate policies or decision making
- Administrative laws attempt to control the actions of these corporations.
- The U.S. Department of Justice is often given responsibility for prosecution.