
Introduction

Jack M. Balkin and Nimrod Kozlovski

As more aspects of our life move to digital networks, crime comes with them. Our lives increasingly depend on the Internet and digital networks, but these create new vulnerabilities and new ways for criminals to exploit the digital environment. Not only can many existing crimes be replicated in online environments, but novel crimes that exploit specific features of digital networks have emerged as well. With new crimes come new forms of policing and new forms of surveillance, and with these come new dangers for civil liberties. These issues are the subject of the present book.

The shift to digital environments alters our understanding of crime in five different ways. First, it alters the scene or location where crimes occur. Second, it facilitates the commission of new types of crimes. Third, it produces significant changes in law enforcement methods, for example, a shift to prevention and to new forms of cooperation between public and private actors. Fourth, it gives law enforcement new tools of digital surveillance and new methods of sorting data and managing online risks. Fifth, it presents new challenges to the existing legal process and spurs the development of new forms of proof and procedure. We have arranged the essays in this book to correspond to these five key phenomena: the *new scenes* of crime, the *new forms* of crime, the *new methods* of law enforcement, the *new tools* of digital surveillance and crime prevention, and the *new procedures* that courts and legislatures will have to adopt to deal with threats to Internet security.

The essays in Part I describe the new crime scene—the digital networked environment. Online criminal behavior exploits the physical and social features of the Internet. Five key features of the online world create new security risks and shape the kinds of criminal behavior we find there.

The first is *digitization*—common standards for data transmission that enable manipulation and modification. The second is *anonymity*—the ability to act and spy on others without disclosing one’s identity. The third is *interconnectivity*—the fact that everyone on the network is connected to everyone else. The fourth is *decentralization*—the lack of centralized control over digital networks. The fifth is *interdependence*—the shared vulnerabilities that inevitably exist between and among all the people who use digital networks.

Digitization, anonymity, interconnectivity, decentralization, and interdependence structure the online world as we currently know it. Hence they structure the opportunities for crime and the ways that people commit crimes and breach network security. However, the task of cybercrime policy is not simply to create new laws banning new practices. It also requires us to redesign digital architectures to reduce the risk of criminal conduct and security breaches in the first place; this requires policy makers and technologists to decide how we should shape the digital networked environment.

Dan Geer’s essay, “The Physics of Digital Law,” introduces some of the basic problems of cybersecurity. When addressing the dangers and risks inherent in the digital environment, he argues, our everyday intuitions are likely to fail us. The physics of the digital environment is quite different from the physics of the offline world. In cyberspace, events occur almost instantaneously across large distances, network boundaries do not align with physical and political boundaries, and everyone on the network is your neighbor. In the digital environment copying is costless, the cost of data acquisition approaches zero, and it is easier to retain information than to delete it selectively. Digital environments are subject to attacks from a wide range of locations, including machines of unsuspecting users that have been commandeered by attackers; and successful attacks can have systemwide repercussions. Geer argues that the new physics of the virtual environment will reshape legal concepts like jurisdiction and ownership; it will require us to rethink doctrines of tort liability and duties of care, and it will revolutionize the way we think about privacy.

Lee Tien points out that the design of software and hardware in networked systems—their “architecture”—is a central device for regulating network activity, one that also has enormous influence on the practical liberty and privacy that ordinary people enjoy. Because architecture is such a powerful method for regulating activity on digital networks, governments will attempt to employ it for their own ends. Nevertheless, Tien

argues, government regulation of digital architecture—for example, by requiring a back door to facilitate government eavesdropping—poses serious problems of transparency, because most people will not be aware of the design or who required it. They will tend to accept the architectural constraints as normal and natural and thus fail to properly contest them as they would laws that restrict their freedom. “Architectural regulation,” Tien points out, “is less visible as law, not only because it can be surreptitiously embedded into settings or equipment but also because its enforcement is less public.”

Tien argues that architectural regulation creates an additional and even more worrisome problem of transparency, particularly where privacy is concerned. Our notions of reasonable expectations of privacy are determined by social norms, which in turn are shaped by our interactions with the technology we see around us. For example, our experience with doors and locks helps us determine when it is reasonable to believe that we will not and should not be disturbed or spied on. Tien worries that if government is given free rein to regulate software architectures in secret it will undermine our experience with the resources necessary to develop privacy norms for the digital age. Because people will not know when and under what conditions they lack privacy, they will not be able to develop the relevant social norms to protect themselves. This is doubly problematic because constitutional rights to privacy depend on these social norms and expectations.

Just as the technical design of security systems has political ramifications, political visions shape technical design, Helen Nissenbaum argues in her essay. She contrasts two current approaches to technological design that flow from two different visions of the problem of cybercrime. The technical community of computer designers and programmers gravitates toward what Nissenbaum calls a model of “technical computer security.” It focuses on protecting computer systems and their users from attacks (and threats of attacks) “that render systems, information, and networks unavailable to users,” “that threaten the integrity of information or of systems and networks by corrupting data, destroying files or disrupting code,” and “that threaten the confidentiality of information and communications.” For the technical community, computer security is about safeguarding systems and creating mechanisms of trust and assurance so that users can use the information they want more or less as they like.

The national security community, by contrast, has a very different vision, which Nissenbaum calls the model of “cybersecurity.” The goal

here is to meet imminent and existential threats to the social order. Officials see the world as rife with conditions that pose immediate and dire threats to the community's very existence and that must be dealt with by whatever means necessary, a way of characterizing the world that Nissenbaum calls "securitization." Because the "cybersecurity" approach sees digital networks as creating potential conditions of catastrophe, it leads to far more extreme responses, and it tends to legitimate special and extraordinary measures that bend the rules and restrictions of normal governance. As applied to computer security, the cybersecurity model calls for centralization of control, technical barricades that prevent access, a shift toward full identification of users, and greater monitoring of traffic. Nissenbaum argues that the choice between these two design visions will be crucial for the digital environment we inhabit in the future, and the rights and liberties we enjoy in that environment. She points out that while securitization might make digital networks marginally safer, the model might succeed at the expense of the Internet's core purpose of providing a relatively uninhibited realm of public discourse.

Part II explores new crimes in the digital networked environment. Anonymity, interconnectedness, and accessibility to vast amounts of information facilitate older crimes and set the stage for new ones, including pure information crimes. Among the activities that governments now seek to prevent are third-party misappropriation of trade secrets over the Internet, economic espionage, unauthorized access to encrypted virtual spaces, computer fraud, and dissemination of circumvention programs. And because the Internet demands ever new forms of authentication to conduct business, new forms of identity theft have emerged. The central questions now are whether extending traditional criminal remedies to new crimes is the right solution; whether civil remedies or technological solutions might be more effective; whether pure information crimes need to be dealt with differently than other kinds of crime; and whether legislative expansion of crimes and the growing criminalization of online activity will do more harm than good.

Beryl Howell describes some of the key legal problems through a series of case studies. Her stories show that the law is not always clear about whether specific conduct is a crime, or which tools investigators may legally employ to collect evidence. For example, in regulating computer hacking, the law faces the task of settling upon a definition that can differentiate legitimate from illegitimate access to data. Developments like peer-to-peer (P2P) technology have made it increasingly difficult to define

illegal possession of material such as child pornography. The new information crimes have proved to be a challenge for a criminal law that demands clear lines between the legal and the illegal. Howell contends that many current laws are written far too broadly, with the result that they hamper legitimate attempts at self-help to identify perpetrators of harmful online crimes. She argues that we need more specific prohibitions that clarify the boundaries of illegal conduct and guide law enforcement officials about how to conduct investigations with appropriate respect for civil liberties and privacy. "It would be ironic, indeed," Howell concludes, "if the concern over harmful online activity results in over-regulation of the use of certain technologies with the effect of hamstringing victims and investigators from using those or similar tools to stop or prevent the harmful conduct."

Part III describes new methods of law enforcement for the digital networked environment. The Internet puts into question long-established notions about how to investigate crime and enforce criminal law. It has led to an increasing emphasis on decentralization of intelligence gathering, privatization of enforcement, and delegation of powers to nongovernmental entities. To address the problems of cybersecurity, technologists, businesspeople, and government officials have experimented with public-private collaborations, self-help measures, automated enforcement, community vigilance, and collective sanctions, leading to what may well become a new system of law enforcement. But this new model is not without its own problems. How can we protect civil liberties and constitutional rights when intelligence gathering is decentralized, when prevention and self-help are strategies of first resort, and the criminal law is increasingly enforced by private parties? How will incentives change when sanctions are invisible, decentralized, and privatized? What is the proper role of the community in sanctioning bad behavior and how can we design technology to strengthen appropriate collective enforcement and discourage inappropriate methods? What are the long-term consequences of replacing human judgment and prosecutorial discretion with automated sanctions?

Nimrod Kozlovski believes that we are in the midst of a paradigm shift in law enforcement. The technological and social conditions of criminal activity have changed and the conventional law enforcement response to crime is ill-equipped to address these changing conditions. Law enforcement offline is mainly a reactive system, relatively centralized, publicly managed, and rooted in human discretion. The emerging system of online

law enforcement, by contrast, is largely preventive, strongly decentralized, involves a hybrid of public and private enforcement, and is highly automated. This new model, Kozlovski argues, is influenced by information security strategies. Far more pervasive than traditional offline law enforcement by state actors, it tries to achieve ubiquitous policing of online activities to monitor, control, deter, deflect, detect, prevent, or preempt risky and potentially malicious activities. Kozlovski warns, moreover, that this new system of policing is emerging without a clear legal structure and with few restraints other than the limits on the ingenuity of the persons involved.

The legal, institutional, and technological settings of conventional law enforcement have been based on the conditions of physical crime scenes; they do not translate well to online law enforcement, and so are ill-suited to restrain overreaching and limit illegitimate uses. In a democratic society, Kozlovski insists, those invested with policing power—whether public or private—must be accountable for their activities. This means that they must have a legal responsibility to account for actions taken and actions not taken, and to explain or justify them; in short, there must be an obligation to expose one's policing decisions to review and to the possibility of sanctions for improper behavior. In the online world, Kozlovski argues, civil liberties will best be protected by creating new accountability mechanisms that will deter public and private police from abusing their power, and at the same time promote efficiency and democratic dialogue about how power is exercised. The time to develop such accountability mechanisms is now, when the technology for the new policing model is still being developed.

One of the key features of the new model is self-help, and this is the subject of Curtis Karnow's essay. Karnow argues that the traditional legal system is increasingly incapable of policing online illegal behavior or enforcing its laws. Given the growing threats posed by computer malware and the relative ineffectiveness of the legal and technological responses to them, it is no surprise that people have turned to defensive technologies; and when these have proved unavailing in an increasingly complex networked environment, they have turned to self-help.

Self-help mechanisms try to identify an attack on the network, trace back the source and shut down, or partially disable, the attacking machines. The goal is to minimize the attack and secure the environment. While promising in theory, Karnow argues that there are many practical difficulties. Using current Internet routing protocols, it is often quite diffi-

cult to pinpoint the perpetrator of an attack, causing the risk of disabling or damaging the wrong machine or the wrong piece of code. In addition, some counterstrikes turn out to be far too broad, creating a cure worse than the disease.

Even if these technical problems are surmounted, important legal concerns remain. Many cybercrime statutes make it illegal to attack or disable computers. Although Karnow notes that self-defense may be available in some cases, one would need to establish both good faith and reasonable belief that there were no adequate alternatives to a self-help counterstrike. This burden of proof is likely to deter self-help. A better approach, Karnow argues, is to invoke the common law right to abate nuisances. Internet-mediated attacks, such as viruses and worms, Karnow believes, fit comfortably within the definition of nuisance; moreover, the doctrine permits the defendant to impose a reasonable amount of collateral damage in order to abate the nuisance.

Part IV considers the new tools available to public and private actors to detect, investigate, and prevent criminal behavior. Law enforcement agencies now have at their disposal sophisticated means for surveillance and ever more powerful ways to analyze vast amounts of information. These technological tools can deter illegal activity, investigate crime, collate personal information, and track criminals with increasing efficiency. In addition, advanced analysis software and data mining tools can preempt crimes by identifying suspicious patterns of behavior, allowing private and public actors to neutralize threats before they are realized. At the same time, these new tools create threats to civil liberties, particularly personal privacy. Moreover, new technologies attempt to predict and prevent crime before it occurs. But these technologies raise the obvious question of whether it is wise to delegate social control to automated systems with little possibility of an appeal to human judgment. No computer model is perfect, and the cost of predictive systems may be constraints on individual liberty and sanctions against the innocent.

Kim Taipale argues that the trade-off between privacy and security is largely illusory; the real issue is how to design technologies so that we can enjoy both values. New information technologies hold the promise of analyzing vast amounts of information to identify potential terrorists and to preempt terrorist acts. Nevertheless, Taipale argues that the public anxiety about electronic privacy is out of proportion to the actual privacy risk; moreover, such fears obscure the very real threat posed by our failure to improve security. Privacy, Taipale contends, is less about preserving

secrecy than protecting autonomy, and he suggests how we might design identification systems and data collection techniques to achieve that goal. In particular, Taipale argues that we protect privacy by separating observation of behavior from knowledge of identity. Much data analysis, including list and pattern matching, can be accomplished with anonymized or pseudonymized data. This data can be collected and analyzed to improve security, but kept in a form that does not identify specific individuals and compromise their privacy interests. Legal rules, in turn, can provide procedures to determine when law enforcement officials are permitted to connect particular behavior to a particular person or persons.

Emily Hancock is concerned that the demand for new law enforcement tools can stifle innovation. Her specific focus is the Communications Assistance for Law Enforcement Act (CALEA), which requires telecommunications carriers (including telephone companies) to make it possible for law enforcement officials to intercept communications when they are legally authorized to do so. CALEA was directed at standard telephone service when it was originally passed in 1994. Since then telecommunications technologies have changed rapidly, and now include a wide panoply of services, including VoIP (Voice over Internet Protocol) technologies that use the Internet to make phone calls. Hancock warns that expanding CALEA's reach to include these new technologies carries risks not only for individual privacy but also for innovation. She notes that all technological change affects law enforcement, sometimes rendering existing methods less effective or irrelevant. Nevertheless, she argues, dictating the design of new technologies to facilitate law enforcement has its own costs, and may even be self-defeating; for example, telecommunications innovation will simply move overseas.

Part V considers the new legal procedures and legal sanctions that digital networked environments require and make possible. Inevitably, rules of procedure and evidence will have to adjust to changes in the nature of crime and the nature of law enforcement. For example, cybercrime, like much Internet activity, respects no boundaries, leading to complicated problems of international law enforcement. Geographical rules of jurisdiction do not always follow the geography of information flows. Evidence introduced in court in digital form may lack the necessary authenticity because it is susceptible to manipulation. Conversely, new kinds of sanctions can be invisibly and automatically imposed without human discretion, bypassing the normal criminal procedural protections of the Bill of Rights. These and other changes in the nature of crime and

law enforcement will require governments to adapt—and in some cases reconstruct—criminal procedure to meet the challenges posed by digital networks.

Susan Brenner focuses on some of the international aspects of computer crime through an examination of the Council of Europe's Convention on Cybercrime. The Cybercrime Convention arose to deal with recurring legal problems: Unlike real-world crime, which requires proximity between the perpetrator and the victim, cybercrime tends to operate remotely and to transcend national borders; hence, national laws have often proved inadequate to deal with it. Investigation and prosecution of cybercrime also requires much more robust mechanisms to facilitate cooperation between different countries with different laws and different rules of criminal procedure. Finally, cybercrime investigations are often based on digital evidence that tends to be fragile, volatile, and easily deleted or manipulated.

Although the Cybercrime Convention was drafted to address these challenges, Brenner argues that in many ways it does not go far enough. It continues the tradition of the localized, decentralized system of law enforcement we employ for real-world crime. The convention requires countries to outlaw certain behaviors and to help in international investigations, but it still employs antiquated structures of nationally based law enforcement that are unsuitable for nonterritorially based crime. Brenner concludes that global investigative and law enforcement authorities, or what she calls "a sort of super-Interpol," may ultimately become necessary to deal with the problems of global crime.

Finally, Orin Kerr predicts the development of a special subfield of criminal procedure devoted to cybercrime. Existing rules of criminal procedure, he argues, were naturally tailored to investigations of traditional crimes using physical evidence and eyewitness testimony; they are poorly equipped to handle prosecutions involving primarily digital evidence. Collecting evidence for cybercrimes is so different, in fact, that the older rules of criminal procedure sometimes make little sense. Extraordinarily invasive exercises of governmental power are completely unregulated while comparatively minor privacy concerns can stifle legitimate investigations.

Courts have begun to take tentative steps to create special rules for computer crime cases, but their powers to make new rules are limited, often exercised too late to do much good, and, moreover, are still rooted in a Fourth Amendment jurisprudence designed for physical crimes. Legislatures and executive officials, Kerr believes, are best suited to design new

methods of handling digital evidence and new rules of criminal procedure for computer crimes.

The essays in this book show how the traditional concerns of criminal justice are merging with newer questions of cybersecurity. Many of the key questions of cyberlaw apply here as well: how government officials can regulate a medium that does not respect national borders, the extent to which law enforcement goals are best served by hardware and software solutions, and the unintended consequences of relying on hardware and software architectures rather than legal norms to structure and control social life.

This book presents a snapshot of a rapidly growing and changing field in the first decade of the twenty-first century. Our working assumptions in preparing this volume—that we must recognize new scenes of crime, new kinds of crimes, new methods and goals for law enforcement, and new tools of surveillance and crime prevention—will surely be tested in the years ahead. We can only wonder at how similar the issues will appear a generation hence, and whether the trends we have identified will have become even more pronounced or will have been displaced by still newer and more pressing concerns.