Introduction

The Myth of the Surveillance Panopticon

> The telescreen received and transmitted simultaneously. Any sound that Winston made, above the level of a very low whisper, would be picked up by it; moreover, so long as he remained within the field of vision which the metal plaque commanded, he could be seen as well as heard. There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live – did live, from habit that became instinct – in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized.[1]
>
> George Orwell, *1984*

George Orwell's chilling vision of the future showed how a totalitarian state could use new technologies to destroy privacy and freedom. Orwell wrote the novel in 1948,[2] when computers filled entire rooms, processing data at a snail's pace. Television was in its infancy, and devices like thermal imagers and particle detectors existed only in science fiction.[3] At the dawn of this technological revolution, Orwell presented a clear message: new technologies would allow the state to dramatically increase its power over the individual, enabling totalitarian states to control every aspect of its citizens' lives.[4]

Many people today have come to believe that our world is starting to resemble Orwell's dystopia. They read about law enforcement agents using powerful new surveillance technologies and react with trepidation.[5] Over the last century, the government has tapped our phones;[6] installed video cameras and hidden microphones in our offices, homes, and hotel rooms;[7] intercepted our e-mails;[8] scanned crowds for images of our faces;[9] monitored our web browsing;[10] seized and copied our hard drives;[11] and even looked through the walls of our houses.[12] The National Security Agency runs secret programs using third party companies that collect our e-mails, browsing history, telephone calls, social media, and stored data. Law

enforcement agencies use devices known colloquially as "Stingrays" which can mimic cell phone towers and intercept our telephone calls.[13] Video cameras watch us from fixed locations throughout the city, satellites monitor us from space, and soon drones will fill the skies to monitor our movements.

Politicians,[14] judges,[15] Fourth Amendment scholars,[16] and lay people[17] from across the political spectrum have reacted with anxiety and alarm, calling for greater regulation from courts or legislatures to protect our privacy rights. The message is nearly unanimous: modern technology poses a grave threat to our privacy, and we must act quickly to reign in the overbearing surveillance state.

This book challenges the conventional wisdom and argues that new surveillance technologies are perfectly compatible with strong privacy protections. To achieve this compatibility, modern surveillance techniques require different methods of evaluation and regulation based on a new paradigm that measures the efficiency of the new technology and then compares the efficiency with existing surveillance techniques. Under this new paradigm, we will find many contexts in which new surveillance technology can increase privacy when compared to traditional surveillance techniques. In other contexts, new surveillance methods can provide more security without any significant loss in privacy. But to maximize the efficiency of these technologies, we must adopt a fresh perspective on regulating government surveillance. We must move away from the Orwellian paradigm that views technology as the enemy of privacy rights and find ways to make technology, including surveillance technology, enhance our privacy.

UNPRECEDENTED CHALLENGES TO FOURTH AMENDMENT LAW

Law enforcement surveillance in the United States is regulated primarily by the Fourth Amendment, as interpreted by the courts. Like most constitutional provisions, the Fourth Amendment uses broad language, prohibiting "unreasonable searches and seizures" and requiring a warrant to be supported by "probable cause." The most specific language in the Fourth Amendment states that people should be secure in their "houses, papers, and effects."[18]

The Fourth Amendment arose out of a series of eighteenth-century abuses involving government agents. In two famous British cases from the 1760s, royal agents investigating "seditious libel" against the King entered the homes of pamphleteers and seized all of their papers.[19] Meanwhile, in the colonies, British customs inspectors obtained broad search warrants that allowed them to search any private residence or business for contraband, a practice that led to a number of lawsuits and standoffs between colonists and British authorities.[20] In responding to these abuses, it is logical that the drafters of the Fourth Amendment were concerned specifically with protecting houses and papers.

For over a century after the Fourth Amendment was ratified in 1791, government surveillance was a straightforward affair: there were no actual "police" as we

currently understand the term (the first metropolitan police force was not created until 1844,[21] and the Federal Bureau of Investigation was not founded until 1908).[22] Government agents conducting surveillance were still mostly customs agents looking for contraband. Neither their methods of surveillance nor the places and things they were surveilling changed in any significant way from colonial times. The Fourth Amendment was rarely invoked but worked fairly well when it was, prohibiting government agents from entering a person's home or going through his or her papers without a warrant. The warrants needed to be supported by probable cause – defined as "a reasonable ground of suspicion"[23] that the defendant was guilty.

In the early twentieth century, new technologies began to change surveillance methods. The invention of the telephone allowed individuals to communicate privately with each other from long distances, enabling conspirators to manage their criminal enterprises without leaving their homes. Government agents responded with a new surveillance technique: wiretapping telephones to listen in on these private conversations.

In its initial attempt to apply the Fourth Amendment's eighteenth century language to new technology, the United States Supreme Court failed miserably. The government had wiretapped the telephone of Roy Olmstead, whom they suspected of running a large bootlegging operation. Olmstead argued that the wiretap violated his Fourth Amendment rights. In a 1928 decision, the Court examined the language of the Fourth Amendment and concluded that no search occurred because the government agents had not entered Olmstead's home.[24] According to the Court, "[t]he reasonable view is that one who installs a telephone instrument with connecting wires intends to project his voice to those quite outside, and that the wires beyond his house, and the messages passing over them, are not within the protection of the Fourth Amendment."[25]

Over the next few decades, the Supreme Court struggled to apply the Fourth Amendment to other new technologies. The advent of the automobile allowed criminals to transport contraband quickly and secretly. Law enforcement responded by stopping and searching cars – and all the containers inside the car – without obtaining a warrant. The Court faced a choice: permit this practice and reduce the privacy of everyone in an automobile, or prohibit the practice and allow criminals to freely move contraband out of reach while the police went to a judge for a warrant. Since its first automobile search case in 1925, the Court has struggled with how to apply the Fourth Amendment in this context: it has decided over a dozen cases involving searches of automobiles and their contents,[26] and has overruled its own precedent six times.[27]

As the twentieth century progressed, technological advances began to change surveillance tools as well. Police officers traced suspects with small mobile tracking devices; they employed informants wearing miniature recording devices; they used drug-sniffing dogs; they installed devices that obtained outgoing phone numbers; they flew airplanes and helicopters over homes and businesses, using telescopic cameras to

photograph details on the ground and in backyards; and they conducted mandatory urine testing for drugs on state employees.[28] The Supreme Court had to judge the legality of these searches by applying Fourth Amendment language that was meant to prohibit customs inspectors and British soldiers from ransacking homes. These cases pushed the traditional method of interpreting the Fourth Amendment to the breaking point – and all of these examples are over thirty years old.

The last thirty years have only exacerbated this problem. Technological innovations have given us new ways to communicate and store information and have also given the police new methods of obtaining that information. Private citizens own smart phones, encryption software, and other devices that allow us to convey information in ways unfathomable two centuries ago. We use computers which can hold the equivalent of millions of pages of information, and we store even greater amounts of information in the cloud. We spend hours each day on the Internet, while leaving data trails for others to follow. Law enforcement officials gather information with Internet sniffers, drone-mounted cameras, DNA sequencing, and thermal imagers. Meanwhile, we give private companies billions of pieces of data, which the companies then provide to the government, who process the information with big data algorithms.

The Supreme Court has taken important steps to adapt to these innovations. In the early years of Fourth Amendment jurisprudence, the Court evaluated government surveillance with a formalist binary test. If the government surveillance intruded on the defendant's property rights, the court deemed the surveillance a "search" and the defendant received full Fourth Amendment protections; if the surveillance did not infringe on property rights, it was not a search and was completely unregulated by the Fourth Amendment. In the late 1960s, the Court adopted two revolutionary changes to this doctrine. First, in 1967, the Court adopted a new test for whether a surveillance constituted a "search" by focusing on whether the surveillance violated the defendant's reasonable expectation of privacy.[29] One year later, the Court abandoned its binary "search-or-no-search" rule and created a new legal standard of "reasonable suspicion" for less intrusive methods of surveillance[30] thus creating different tiers of surveillance with different legal standards to govern each tier.

These doctrinal shifts helped the Court navigate the evolving technologies of the late twentieth century, but they are insufficient to address modern surveillance techniques. This book proposes that it is now time for the Court to create a new doctrinal framework, analogous to the bold changes the Court made in the late 1960s. First, the Supreme Court needs to realign its "reasonable expectations of privacy" analysis so that it is more precise and more reflective of what society actually believes is intrusive. Second, the Court must adjust its legal standards to incorporate new quantitative tools that are more and more commonplace in law enforcement investigations, such as big data algorithms that can predict criminal behavior. Finally, the Court must expand the number of legal standards applicable to surveillance so that each standard more precisely matches the level of intrusiveness of the

surveillance. These changes will require the Court to move away from the zero-sum game approach[31] that currently dominates its jurisprudence and evaluate new surveillance methods through a new lens: the cost–benefit analysis theory.

THE ZERO-SUM GAME MENTALITY

Over the past few decades, the Court has generally followed a specific doctrine known as the "equilibrium adjustment theory" when applying the Fourth Amendment to new technologies.[32] The equilibrium adjustment theory is based on a fundamental truism of criminal procedure: that the goal of policymakers is to strike the appropriate balance between liberty and security. The underlying assumption is that there is, and always will be, a trade-off between liberty and security, and the only way to get more security is to forfeit some liberty. The job of the courts is to mediate that struggle, to be referees in the "game" of cat-and-mouse between the police officer and the criminal. Before the Fourth Amendment was written, the parameters of the game were well-established by Benjamin Franklin, who declared: "[t]hey who can give up essential liberty to obtain a little temporary safety, deserve neither liberty nor safety."[33]

Judges frequently refer to criminal investigations as a competitive enterprise, in which the job of the courts is to maintain the equilibrium between both sides. The Supreme Court has repeatedly stated that the purpose of the Fourth Amendment is to act as a safeguard against the law enforcement officer "engaged in the often competitive enterprise of ferreting out crime."[34] In a seminal article in the *Harvard Law Review* setting out the equilibrium adjustment theory,[35] Professor Orin Kerr argued that "the basic dynamic of Fourth Amendment law resembles a zero-sum game,"[36] and asserted that the fundamental principle driving Fourth Amendment jurisprudence over the past hundred years has been the courts' desire to maintain an "equilibrium" between police power and civil liberties.[37] As new technologies are developed and put into use by criminals or by law enforcement officials, the equilibrium is disrupted, and the law must adjust to restore the appropriate balance.

This zero-sum model can be represented by a one-dimensional graph, with privacy on one end of the spectrum and security on the other end of the spectrum. The first step requires the society to decide where it wants to set the original balance:

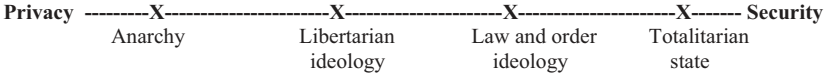

FIGURE 1

Professor Kerr sets the balance by imagining a "Year Zero," an imaginary time when police investigated crime without any special investigatory tools, and when criminals committed crime without any special technologies to aid them.[38] The goal of the equilibrium adjustment doctrine is to ensure that the balance between security and

privacy remains. Assume the balance between privacy and security at Year Zero fell somewhere close to the middle, perhaps leaning somewhat towards privacy rights:

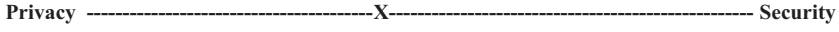

FIGURE 2

Assume that a technological innovation arises that increases privacy, such as the automobile.[39] When compared to Year Zero, individuals can now transport themselves and their cargo quickly and in relative secrecy, which increases privacy. Criminals also get the benefit of this technology, making it easier for them to avoid detection, which decreases security. Now, in situations where suspects use automobiles, the balance has shifted towards privacy rights, and away from security. This disrupts the equilibrium:

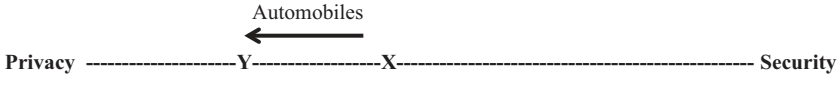

FIGURE 3

The law then reacts – in this case, by loosening the rules on surveillance to allow police to search cars without a warrant.[40] This change restores the equilibrium to (roughly) the level it was at Year Zero:

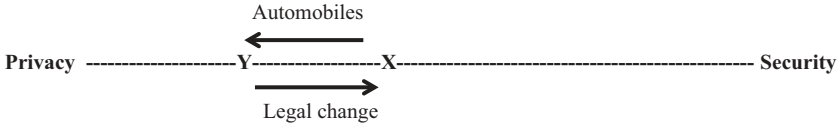

FIGURE 4

This equilibrium adjustment process occurs with every type of new technological innovation that individuals (and criminals) use to increase their privacy, such as telephones[41] or personal computers. It also applies to new technological innovations that increase the government's surveillance power. For example, assume the government begins to use thermal imagers to detect the heat patterns emanating from a home.[42] These devices increase security by helping police detect the presence of heat lamps, which criminals can use to secretly grow marijuana indoors. But they also reveal some intimate details about the home that police could not have known in Year Zero without entering the home.[43] Thus, the courts will intervene with a new legal rule: the police may not use a thermal imager unless they first obtain the warrant. This warrant requirement means that the interior of the home has as much privacy as it did in Year Zero. It also neutralizes the security benefits of the new surveillance technology: we are at exactly the same level of privacy and security as we were before this new surveillance technology was invented. This demonstrates how the equilibrium adjustment theory always provides a

zero-sum result; we can never improve our security nor lose any privacy when applying this theory.

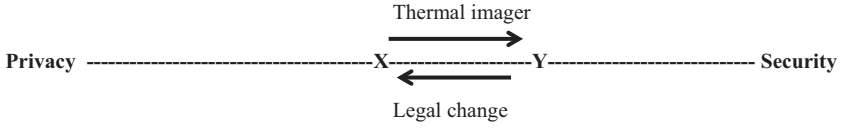

FIGURE 5

A NEW PARADIGM

The equilibrium adjustment theory is relatively simple to apply and it appeals to our sense of fairness; after all, what could be more fair than to maintain the balance that we have lived with for decades? But as societal and technological changes become more pronounced, certain flaws in the equilibrium adjustment theory become apparent.

The first problem is the absence of any normative proof that the balance of "Year Zero" is the right balance. Professor Kerr envisions Year Zero as a time before criminals or police were able to use tools to commit or investigate crime. The Supreme Court appears to have set Year Zero as the date when the Fourth Amendment was adopted; in a recent case, the Court stated that "we must assure [] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted."[44] Either way, the goal of the equilibrium adjustment theory is to return us to the balance that existed between privacy and security in an era over two hundred years ago.

There is no reason, however, to believe the balance of that era was the optimal balance for society. [45] Even if Year Zero did feature the ideal balance between privacy and security at the time, that ideal balance may have evolved as society changed. In Year Zero, for example, it may have been sensible to create a rule that an individual surrenders all Fourth Amendment rights in information that shared with third parties. If you write a letter to your friend detailing your plans to kill your neighbor, and the friend then decides to share the letter with the police, it would make no sense for you to claim that the government was violating your Fourth Amendment rights by reading the letter. But in modern society, we unavoidably reveal vast amounts of information to hundreds of private corporations, and many of us believe that this information deserves some privacy protections. Thus, changes in technology and in society will alter the optimal balance between privacy and security. The equilibrium adjustment theory has no way of accommodating that changing standard; it will always assume that Year Zero's balance for third-party information is optimal.

Similarly, changes in society or technological advances may result in an *increased* need for security in certain areas. For example, at Year Zero, it was illegal to search a suspect without some evidence specific to the suspect that he was committing a crime. Courts have generally adhered to this rule, known as the individualized suspicion

requirement. But after a series of airplane hijackings in the late 1960s, the federal government in 1970 instituted mandatory searches of all individuals who were about to board an airplane, with no individualized suspicion requirement.[46] If courts had blindly followed the equilibrium adjustment theory, they would have struck down these searches to restore the balance from Year Zero. But in evaluating these cases, courts refused to follow the equilibrium adjustment model and instead recognized that the new danger posed by hijackers required a change in the balance between privacy and security in this context. These courts have permitted suspicionless airport searches even though they do not neatly fit into Fourth Amendment doctrine.

The second and more fundamental problem with the equilibrium adjustment theory is that it adopts the traditional zero-sum paradigm involving privacy and security. But there is not always a one-for-one trade-off between privacy and security. It is possible, in other words, to increase privacy without affecting security; or, conversely, to increase security without affecting privacy. To illustrate, we need to stop thinking about privacy and security as opposite poles of a single axis, but instead as two independent variables on a two-dimensional graph. This two-dimensional graph will still contain our initial line showing the trade-off that usually occurs between privacy and security, as in our automobile example.

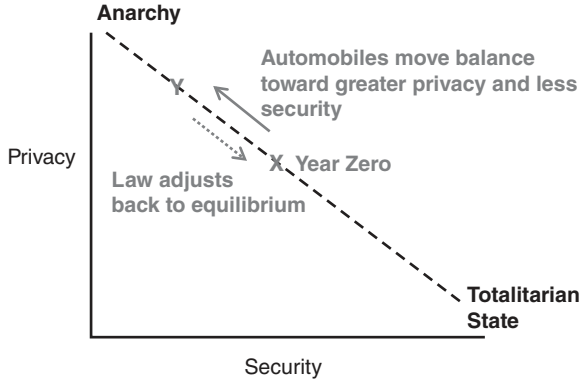

FIGURE 6

In the automobile example, the balance between privacy and security remains on the zero-sum line, reflecting that in this situation there can be no gain to privacy without a loss to security. But this new, two-dimensional representation allows us to contemplate situations in which there is not a one-for-one trade-off between security and privacy; situations in which one value can increase while the other stays constant, creating a positive-sum game.

A positive-sum change can occur because of a technological advance. For example, assume that law enforcement agents searching for firearms can use metal detectors instead of subjecting individuals to a pat-down. The metal detectors are just as accurate in detecting firearms, so there is no loss in security, but the privacy intrusion is much lower, so individuals experience an increase in privacy.

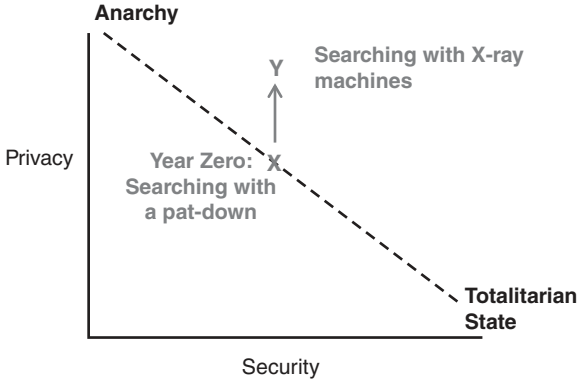

FIGURE 7

Another example involves so-called Internet sniffers. These are software programs that can search through immense amounts of data looking for specific key words and images. Imagine that a law enforcement agent believes that a suspect is guilty of distributing child pornography through e-mail. The agent could look through all the suspect's e-mails for the next few months to see if there are any child pornography attachments. This would be an effective method of detecting criminal activity, but it would come at a very high price to the suspect's privacy. Whether the suspect is guilty or innocent, the agent will have inspected a large amount of private communications.

Now assume that the agent instead installs an Internet sniffer on the suspect's email account and programs the sniffer to only alert the agent if the sniffer finds a child pornography image. The level of security will be the same: if the suspect transmits child pornography, the agent will know about it. But the privacy intrusion will be much less, since the agent will learn nothing else about the suspect's e-mails (and if the suspect is in fact innocent, the agent will learn nothing at all about the suspect's e-mails).

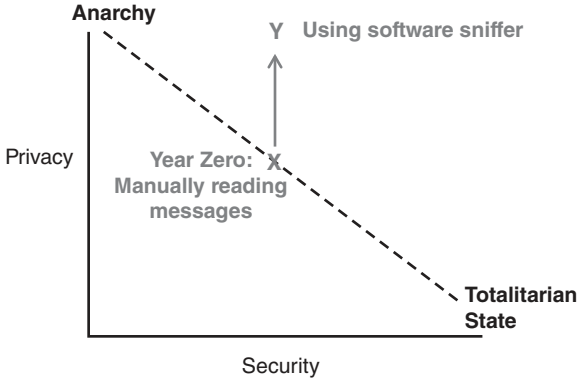

FIGURE 8

Other technological changes, from big data algorithms to gun detectors to continuous GPS monitoring, have created the possibility of similar positive-sum changes.

But they also raise important and challenging questions about how best to regulate these new technologies, such as whether to consider the economic cost of the surveillance method or the severity of the crime being investigated.

In order to improve on the equilibrium adjustment theory, our new paradigm must be dynamic, in the sense that it needs to respond to changing expectations of privacy or new security needs. In order to achieve that flexibility, it needs to be able to measure both the level of intrusion posed by different types of surveillance and the security benefits that the surveillance provides. Finally, the paradigm needs to acknowledge that the trade-off between privacy and security is not a zero-sum game, and it ought to encourage surveillance methods that allow for a positive-sum change. The cost–benefit analysis theory proposed in this book meets all of these criteria. It represents a fundamental rethinking of how courts approach this problem, but the proposed changes are no more radical than the changes the Supreme Court made in the late 1960s when it adopted the *Katz* "reasonable expectation of privacy" test and created different tiers of surveillance in *Terry* v. *Ohio*.[47] In fact, many facets of the cost–benefit analysis theory are updates to these earlier changes: the theory requires us to measure reasonable expectation of privacy (and other levels of intrusiveness) with greater precision and creates more tiers of surveillance to reflect the realities of modern surveillance.

MOVING FORWARD

The first section of the book will describe the cost–benefit theory. Chapter 1 introduces the theory by examining how to measure the costs of different types of surveillance, particularly the cost to our privacy. Currently the Supreme Court determines these costs, but the Court is poorly situated to make these determinations. Under the current regime, the Court usually only rules on whether the intrusiveness of a particular surveillance exceeds a certain threshold of intrusiveness – that is, whether the surveillance is a "search." But the cost–benefit theory requires a more precise calculation of the level of intrusiveness; it requires a measurement of the degree to which the surveillance infringes on our privacy. Furthermore, the Supreme Court decides only one or two cases a year on this issue, which is insufficient to keep up with the multitude of new types of surveillance that occur in modern investigations.

Chapter 2 focuses on the benefits side of the equation and notes that the rise of big data's predictive algorithms allows law enforcement to measure the likely success rate of surveillance with far greater precision than previously possible. These predictive algorithms have the potential to revolutionize criminal investigations in many ways, making them cheaper, more accurate, and less biased. However, surveillance technologies must be designed in ways to ensure that they meet the Fourth Amendment's requirement of particularized suspicion and to ensure that they do not rely on tainted data.

In Chapter 3 the book addresses another challenge of applying the cost–benefit analysis theory: how to incorporate quantified costs and benefits into a legal system that currently uses broad, descriptive standards to evaluate searches. We will see that descriptive standards are inconsistently applied in their current form, and thus provide inadequate guidance for police attempting to follow them. The chapter also points out the dissonance between the manner in which judges apply the current standards and the way in which lay people believe the standards should be applied. Quantifying the applicable legal standards will make the standards more transparent and allow judges to apply a greater range of standards. Quantification will also allow judges to use the results of predictive algorithms as formal factors when evaluating the legality of particular forms of surveillance.

The next section of the book applies the cost–benefit analysis theory to various methods of technology-enhanced surveillance. The book divides these surveillance methods into four broad categories: reactive surveillance, in which the government adopts new surveillance technologies in order to keep up with privacy-enhancing technology; binary searches, which collect information without infringing on legitimate privacy rights; mosaic searches, which collect and process massive amounts of publicly available information; and hyper-intrusive searches, which allow the government to detect our most private, intimate information.

Chapter 4 begins by examining reactive surveillance, such as thermal imagers, decryption tools, and devices that reveal the phone numbers that are being dialed on a telephone. These are tools which the government needs in order to respond to privacy-enhancing technology used by private citizens. Although reactive surveillance tools can be very intrusive, in most contexts they are only being used to learn information that would ordinarily be public but has been hidden by new forms of privacy-enhancing technology, such as heat lamps, cell phones, and encryption tools. In evaluating reactive surveillance, we need to consider both the level of criminal activity that is potentially masked by the privacy-enhancing technology, and how the privacy-enhancing technology has affected society's expectations of privacy. In the context of encryption, we need to assist law enforcement even further, by creating a key escrow system which will give law enforcement the ability to decrypt any piece of data upon obtaining the proper legal authority.

Chapter 5 describes a uniquely productive type of surveillance known as a binary search. Binary searches reveal no information other than the absence or presence of illegal activity. The Supreme Court has determined that a binary search does not implicate the Fourth Amendment, since an individual does not have a legitimate expectation of privacy in illegal conduct. The cost–benefit analysis theory encourages binary searches, because they are the archetypal example of positive sum surveillance: if designed properly, they can increase the level of crime detection without increasing the level of privacy infringement. Soon facial recognition technology and advances in crime recognition software will allow law enforcement to achieve nearly 100% enforcement for certain crimes. Such a development, though

theoretically desirable, has potentially negative side effects, especially in the current environment of overcriminalization.

Chapter 6 examines mosaic searches, and discusses the potential and challenges created by big data surveillance. Recent developments in surveillance technology allow police to engage in various methods of widespread, low-cost surveillance, from tracking a person's location through her cell phone to predicting behavior based on a person's telephone records, credit card purchases, and other publicly available details. Data points will only become more numerous in the future, as camera-mounted drones and self-driving cars become common. Courts and legislatures have been wary of these widespread surveillance techniques, and in fact have sought to restrict them because their financial cost is so low that they allow law enforcement to engage in nearly indiscriminate surveillance. But the cost–benefit analysis theory shows that courts should adopt the opposite approach: all other factors being equal, a surveillance method that is less expensive should be encouraged, not restricted. Furthermore, encouraging low-cost widespread surveillance will help to even out the massive inequities we now see in government surveillance, where the poor and people of color bear a much greater cost than more enfranchised and less surveilled citizens. Finally, applying the cost–benefit analysis theory will require the government to demonstrate the benefits of indiscriminate surveillance, which will encourage the government to develop and utilize more productive (and less intrusive) methods of surveillance.

Chapter 7 explores a specific aspect of mosaic searches: information that individuals turn over to private companies. Under the controversial third-party doctrine, individuals surrender all Fourth Amendment rights when they share information with a third party. In modern society, we routinely share vast amounts of private information with a variety of companies and organizations; this trend will accelerate with the emerging technology of smart devices and the "Internet of Things." These developments have led most legal scholars to criticize the third-party doctrine as anachronistic and a significant threat to privacy. This chapter will argue that the conventional wisdom is wrong for two reasons. First, modern information sharing enhances our privacy; thus, some aspects of the third-party doctrine can be classified as reactive surveillance. But more importantly, the cost–benefit analysis theory reveals that this massive private collection could result in a positive-sum shift in surveillance. On the privacy side, corporations themselves can assert their own Fourth Amendment rights to keep this information secret – a phenomenon we are already seeing in many technology companies that store and transfer our data.[48] On the security side, millions of companies are constantly collecting billions of pieces of data, all of which can be available to help solve crimes when the government can meet the appropriate standard to overcome the companies' Fourth Amendment rights.

Chapter 8 discusses the final category of technology enhanced surveillance: hyper-intrusive searches. These searches occur when law enforcement agents use surveillance technology to see and hear private, intimate information that would

otherwise be undetectable. This category includes video monitoring of private places and real-time interception of oral or digital communication. This type of surveillance unquestionably needs greater regulation; the question is what form that regulation will take. This chapter reviews the variety of different tools that courts have at their disposal to regulate hyper-intrusive searches and examines which of these tools will make these searches more productive.

The primary theme of this book is that we should not regard new technology as an enemy to privacy, even when the government is wielding it as a surveillance tool to investigate crime. Our own use of technology has already enhanced our privacy considerably and will continue to do so, and with the appropriate regulatory paradigm, the government's new surveillance tools can dramatically enhance our security with minimal effect on our privacy. The first step in developing this regulatory regime is to move away from the zero-sum game that currently dominates the Court's analysis. Therefore, we will begin our discussion by proposing the cost–benefit analysis theory as the fundamental basis for regulating government surveillance.