Identifying Terrorists: Privacy Rights in the United States and the United Kingdom

Joyce W. Luk
Identifying Terrorists: Privacy Rights in the United States and the United Kingdom

By Joyce W. Luk*

Introduction

While the privacy concerns raised by technological advances are widely recognized, recent terrorist attacks and developments in surveillance and information technologies have led to a convergence of technologies that in many situations present a new challenge to the right to privacy.

A. Big Brother Is Watching

Recently, in light of the September 11, 2001 terrorist attacks in New York and Washington, D.C., the government implemented heightened security measures in airports, on bridges, and in federal buildings. In Fresno, California, these security measures included, for the first time in a United States airport, use of facial recognition technology to scan faces for terrorists as passengers entered security checkpoints.1

Earlier in 2001, police video cameras focused on the faces of Super Bowl fans as they streamed through the turnstiles at Raymond James Stadium in Tampa, Florida.2 Cables instantly carried the images to computers in the control room. In less than a second they were compared with thousands of digital images of known criminals and suspected terrorists.3 Fans never knew they were being watched.4

---

* J.D. candidate, University of California, Hastings College of the Law, 2002.
3. Id.
Today, everyone appears to be watching everyone else. Police cameras capture speeding motorists at busy intersections, casinos use facial recognition technology to identify undesirable patrons, and in the gritty East London borough of Newham, British police installed 300 cameras employing facial recognition technology to survey the town center for criminals.\(^5\)

**B. Expansion of Surveillance Technology Outpaces Fourth Amendment Protections**

In the United States, law enforcement, one of the fastest areas of expansion in the federal government,\(^6\) is adopting military surveillance technologies.\(^7\) Additionally, law enforcement agencies have taken advantage of numerous advancements in civilian surveillance technologies, such as facial recognition technology.

Current U.S. law is ill-prepared to deal with the challenges presented by new surveillance technologies. Currently, federal law places controls over the installation of electronic aural bugging devices in private dwellings, but no equivalent statutes address the similar placement of video surveillance devices.\(^8\) This is particularly significant because after the September 11 attacks, the trend of using surveillance technologies is likely to increase even more rapidly.

**C. Thesis**

If properly regulated, the use of video surveillance and facial recognition technologies for law enforcement can be effective in ensuring the safety of citizens while at the same time maintaining an individual's right to privacy. These types of surveillance technologies, when used for proper purposes, are relatively non-invasive and will not inordinately intrude on individual privacy. The use of video

\[^4\] Id. In an interview on CNN Talkback Live, Joe Durkin, a spokesman for the Tampa Police Department, asserted that there were posted warnings throughout the exterior of the football stadium indicating the presence of closed-circuit television surveillance. Furthermore, the cameras were apparently in plain view, thus, the videotaping was not entirely secret. CNN Talkback Live: Should People Who Are Criminals Be Under Surveillance? (CNN television broadcast, Feb. 1, 2001) (transcript no. 01020100V14).

\[^5\] Slevin, *supra* note 2.


\[^7\] Id. at 41.

surveillance and facial recognition technology is justified for the purposes of decreasing crime and preventing further terrorist attacks. However, there should be specific legal protections regulating the proliferation of these new technologies before the technology gets beyond our control.

Currently, under U.S. law, it is unlikely that the use of video surveillance for law enforcement purposes is illegal or unconstitutional per se, even when used in conjunction with facial recognition and information technology. However, this use of technology presents several constitutional issues, particularly the chilling of personal autonomy and the individual's First Amendment right to freedom of speech and association.

In addition to the constitutional issues, there are social and ethical issues that merit consideration. The discourse asks whether people are willing to live their lives under the watchful lens of a video camera, and if so, to what extent they are willing to sacrifice personal autonomy and risk governmental abuse of this data.

Lawmakers should not be deterred from incorporating this new technology to ensure the safety and well-being of its citizens. At the same time, however, unless Congress modifies the law to address the issues raised by new technologies, the public's right to privacy will be severely diminished.

D. Structure of this Note

Parts I and II give a general background on video surveillance and facial recognition software and discuss the technology behind, and uses of, closed circuit television (CCTV) in the United States and elsewhere. These two sections discuss the emerging technologies driving facial recognition applications, their use in conjunction with video surveillance, and the development of other surveillance technologies such as biometric identification and scanning devices.

Part III explores the meaning of privacy, privacy rights, and their applicability to facial recognition technology, video surveillance, and other emerging surveillance technologies in the United States. This section also analyzes the legal and statutory development of privacy rights and explores whether video surveillance incorporating facial recognition technology is incompatible with judicial and legislative

---

9. Video surveillance is normally conducted through CCTV systems. A CCTV system can be as simple as a single camera, monitor and a recorder.
history.

Part IV discusses privacy rights and statutory regulations in the United Kingdom dealing with new surveillance technology.

Part V is a comparative analysis of the privacy protections of the United Kingdom and the United States and includes a proposal implementing some of the United Kingdom's privacy protections in the United States.

Finally, Part VI concludes that proper regulation would allow facial recognition software and video surveillance to be used in ways that help society, without violating personal autonomy and a person's reasonable expectation of privacy. It is unlikely, however, that the United States will implement any proactive legislation to handle the privacy problems created by emerging technologies.

I. Video Surveillance

A. Current State of Video Surveillance

Video surveillance technology and CCTV systems were first introduced in 1956. Thanks to numerous technological advances in recent years, it has evolved to include digitization and miniaturization.

The digitization of images allows for the easy and inexpensive reproduction and transferability of video images. It also allows the digital data representing these images to be stored easily for an indefinite period of time.

In recent years, miniaturization has diminished the cost and size of video surveillance equipment, allowing law enforcement and private consumers increasingly to utilize and/or replace old equipment with the newer more clandestine and unobtrusive technology. For example, pinhole video cameras are now available that fit in the palm of one's hand and can be hidden almost anywhere, even on a watch face. When used in conjunction with remote identification systems, these cameras can return identification

12. Id.
information to the surveillant wirelessly and in real time.\(^\text{15}\)

\section*{1. United States}

Over sixty urban centers in the United States use video surveillance in public places for law enforcement purposes, such as prevention of traffic violations.\(^\text{16}\) Tacoma, Washington, is believed to be the first city in the country to announce publicly that they use video surveillance for law enforcement purposes; Baltimore, Maryland, has what is considered to be the most expansive video surveillance system in the United States.\(^\text{17}\) Recently, Yosemite International Airport implemented biometrics to scan faces for terrorists as passengers enter security checkpoints.\(^\text{18}\)

Television broadcasters and viewers in the United States seem captivated by the vicarious thrill of witnessing invasions of others’ privacy. “Real life” television programming uses video surveillance and CCTV systems to create programs such as COPS and Rescue 911.\(^\text{19}\) Investigative news programs use hidden cameras, while local network affiliates replay footage of criminal activity from police and liquor store video cameras on their news broadcasts.\(^\text{20}\)

There is a recent explosion of “reality-based” television programs, which employ the concept of watching individuals’ everyday activities and unscripted interactions. Participants of these shows—Real World, Survivor, and Temptation Island, for example—clearly have no expectation of privacy.\(^\text{21}\) These shows reflect a trend towards decreased expectations of privacy in the technological age. Their popularity suggests that whatever the rationale, society

---

16. Boal, supra note 13, at 38.
18. Steinberg, supra note 1.
20. Id. at 1108.
21. Reality television programming is popular on the various networks. For example, the Real World (1992-present) is an MTV television series that chronicles the lives of groups of young adults living together. Survivor (CBS 2000) made a big splash over the summer as it followed the trials of a group of adults stranded on an island. The last one left on the island receives one million dollars. Temptation Island (Fox 2001) is based on the same concept as Survivor, except that it involves the seduction of supposedly secure couples by a group of attractive singles in a tropical paradise.
currently has a desire to gaze and be gazed upon.

2. United Kingdom and Abroad

Video surveillance has long been a way of life for much of Europe. In the United Kingdom, CCTV and video surveillance is commonplace. Currently, over seventy-five cities use it to monitor urban centers, and approximately 95% of all local governments are considering its use as a law enforcement tool. Elsewhere, authorities in France, Australia, Ireland, and Scotland use video surveillance in public places as a law enforcement tool.

Cities in Europe that have installed video surveillance cameras claim dramatic reductions in crime rates. Newham, England, one of the first cities to introduce CCTV systems in 1992, has spent more than $30 million installing thousands of street corner surveillance cameras. The city credits these cameras with causing a 13.4% drop in regional crimes. Research on Newham's crime statistics showed an 11% decline in assaults, a 49% drop in burglary, and a 44% drop in criminal damage through the end of 1994 due to the implementation of street surveillance.

B. Uses of Video Surveillance

1. Law Enforcement and Crime Prevention

Law enforcement agencies use video surveillance both as a method to identify criminals and as a tool for crime prevention. These agencies also use clandestine video surveillance to build cases against criminal suspects. Police use police-operated camera systems (in those areas where they exist) and privately operated surveillance systems to identify those who engage in criminal activity.
Police in a number of cities utilize video and camera surveillance to prevent traffic violations and to catch violators. In San Francisco and Los Angeles, authorities positioned cameras at certain street intersections to enforce stoplights by capturing license plate images. Drivers who run a red light can expect to receive a citation in the mail. Elsewhere, the same mechanism enables video and camera surveillance to enforce speed limits. In Scotland, for example, there are an estimated 10,000 cameras monitoring traffic speed and parking structures.

2. Other Uses

In addition to law enforcement, large companies and businesses use video surveillance for a variety of other purposes. They use hidden cameras to monitor employee productivity, deter theft and fraud, and ensure safety in the workplace. Retailers use video surveillance in their loss-prevention programs, and fans of spy literature or films are familiar with the ways in which video and camera surveillance has been used for purposes of espionage.

Voyeurism also drives many applications of video surveillance technology. Video from hidden cameras (e.g. toilet cams, gynocams, and even dildocams!) commonly ends up on the Internet, often depicting women caught unaware.

II. Facial Recognition Technology

Facial recognition technology is a relatively unobtrusive and non-invasive system of biometric identification. A number of corporations design software applications for this technology. The
software uses algorithms to recognize and then represent patterns and relationships in human facial features,37 similar to the way the human brain recognizes and remembers facial images.38 It can locate and identify human faces from live video or static images, at angles of up to thirty-five degrees, while compensating for lighting conditions, skin color, eyeglasses, facial expressions, facial hair, and aging.39 The software is capable of building a time stamped database of facial images for storage, later analysis, and comparisons.40 Facial recognition technology may be used to search watch-lists, video libraries of individual images (such as high school yearbooks, drivers’ licenses, or passport photographs) or law enforcement databases.41 The software does not give 100% probability, rather it lists probabilities based on how confident the system is of a correct identification.42 The system will discard faces that do not match those in the database.43 The limiting factor, therefore, in facial recognition technology is the database. In order for the technology to be effective, governmental databases, perhaps worldwide, would need to be merged.

Authorities can use facial recognition technology in combination with other biometric information, such as fingerprint or retinal scanning.44 Biometric data can also be correlated with an array of personal information, such as an individual’s medical history, tax records, criminal arrest records, voting records, political affiliations, and any other conceivable type of information.45 For example, facial recognition technology recently helped Mexican election officials prevent voter fraud.46

38. Id.
39. Id.
40. Id.
42. Id.
43. Find Criminals, supra note 37.
A. Uses of Facial Recognition Technology

There are two main uses for facial recognition technology: identification, and access control or authentication.47

1. Identification

Identification is the ability to identify one person among those whose biometric identifying patterns have been recorded.48 Law enforcement agencies are able to use facial recognition software to identify criminals or known terrorists by taking video surveillance images and using facial recognition software to identify perpetrators.49 Similarly, they can identify known criminals through active scanning of facial images and simultaneous comparison to a database of compiled facial images.50 Technology that can simultaneously scan facial images and compare those images with others already entered and indexed in a database gives officials the ability to immediately identify known criminals and prevent future crime.51

2. Authentication

Authentication is the ability to verify a person’s identity through a comparison with their previously recorded biometric measurements.52 Facial recognition technology is a useful tool to control access and verify authorization in a number of different areas. Government agencies such as the Department of Motor Vehicles use it to verify vehicle ownership, while financial institutions use it before providing account access.53

For authorization purposes, facial recognition technology is the least obtrusive or invasive of all the biometric technologies. It is equally effective in allowing for quick scanning of large numbers of persons from a safe distance and without the subjects’ knowledge.54

47. Woodward, supra note 44, at 100.
48. Id.
49. Carney, supra note 41, at B1.
50. Id.
52. Woodward, supra note 44, at 100.
B. Other New Surveillance and Information Technologies

In the arena of biometric identification and scanning, the number of technologies currently emerging is impressive. The old standard of fingerprint identification has been improved, supplemented and sometimes supplanted by new technologies using algorithms to compare measurements of individuals' hand features.\(^5\) In fact, a person's fingerprint can now be used instead of a credit card to make purchases.\(^6\) In addition, technology is also available for voice recognition, signature recognition, hand vein mapping, iris recognition, and retinal scans.\(^7\) The first iris-scan-protected ATM in the nation was introduced in Texas in 1999.\(^8\)

The military uses new surveillance technologies such as Forward Looking Infrared Device that detects infrared heat emissions, back-scattered x-ray imaging (which digitally enhances a sketched outline of an individual's body), passive millimeter wave imaging (which can be used to see through an individual's clothing to detect weapons and other items), and radar skin scanning (which is an even more accurate way of scanning an individual's body and discerning weapons carried).\(^9\)

The field of information technology is evolving. For example, data mining, also known as knowledge discovery in databases,\(^10\) compiles a simple recommendation list from gigabytes of structured data, finding patterns that are impossible to anticipate.\(^11\) Researchers, however, have begun to move beyond the original focus on highly structured, relational databases to the areas of text data mining and video mining.\(^12\) Text data mining involves extracting unexpected relationships from huge collections of free-form text.\(^13\) Video mining uses a combination of speech recognition, image understanding, and natural-language processing techniques to open up the world's vast

---

55. Woodward, supra note 44, at 104.
56. Steinberg, supra note 1.
57. Woodward, supra note 44, at 104.
59. Hansen, supra note 17, at 44-45.
61. Id.
62. Id.
63. Id.
video archives to efficient computer searching.\(^{64}\)

The results are still preliminary, but it is conceivable that data mining, when used in conjunction with surveillance and facial recognition technology, could have a powerful impact on privacy rights.

III. The Right to Privacy in the United States

The high regard for privacy in the United States has always been juxtaposed with "a desire to regulate moral life, a suspicion of secrecy, [and] a democratic impulse to openness."\(^{65}\) Surveillance technology raises privacy concerns perhaps more directly than other types of technology because it is designed to enable a surveillant to observe without obtaining consent from the subject.\(^{66}\) Furthermore, although privacy concerns stemming from surveillance activity traditionally involve government intrusion, private actors increasingly have access to surveillance equipment and the ability to invade an individual's privacy.

A. History

In the seventeenth century, the concept of privacy in the American colonies was undeveloped.\(^{67}\) Homes were often small and cramped, making it difficult to maintain privacy.\(^{68}\) Further, in Puritan New England, neighborly spying was seen as a civil obligation, necessary for an orderly society.\(^{69}\)

During the eighteenth century as the United States became more cosmopolitan, a gradual distinction between public and private began to emerge.\(^{70}\) Residences were more spacious and had separate rooms and walls.\(^{71}\) The Constitution protected those homes from unreasonable searches and seizures, and the quartering of troops.\(^{72}\)

---

64. Id.
66. Although surveillance techniques certainly can be used to observe a subject's public activities, new technology can create difficulties in demarcating those activities that are public and those that are private.
67. Horn, \textit{supra} note 65, at 59.
68. Id.
69. Id.
70. Id.
71. Id.
72. U.S. CONST. amend. IV.
During the nineteenth century, journalistic invasions of the privacy of public figures were commonplace.\(^{73}\) The advent of quick photography and mass-circulation newspapers in the latter part of the century gave rise to the United States’ first “invasion of privacy” lawsuits.\(^{74}\) During the Cold War, the government stepped up surveillance of individuals in the name of national security; essentially private matters, such as sexual orientation and membership in “subversive” political organizations, became the basis for accusations of treason.\(^{75}\) Ironically, while suburbia and the automobile increased personal autonomy, Cold War tensions made it increasingly necessary to find out what one’s neighbors were doing.\(^{76}\)

Today, battles over privacy reflect historical conflicts.\(^{77}\) There is always tension between the individual’s need for privacy and autonomy, and the sense that society suffers when morality goes unregulated.\(^{78}\) Of course, society is also thought to suffer from excessive public exposure of private impulses.\(^{79}\) Television and the video camera erase the lines between the public and private, allowing private lives to be put on public display.\(^{80}\)

**B. Interests in Privacy**

Privacy is an essential element of a free society. Without the ability to interact with one another in private, individuals cannot exchange ideas freely. This “marketplace of ideas” is essential for a democracy to function properly, and gives rise to a free society.\(^{81}\) Although no “universally accepted definition of the right to privacy” exists, court opinions that address privacy issues often encompass three types of privacy interests: autonomy, intrusion, and information privacy.\(^{82}\)

\(^{73}\) Horn, *supra* note 65, at 57.
\(^{74}\) Id.
\(^{75}\) Id. at 58.
\(^{76}\) Id.
\(^{77}\) Id.
\(^{78}\) Id.
\(^{79}\) Id.
\(^{80}\) Id.
\(^{81}\) Abrams v. United States, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting) (disagreeing with the majority’s intent test and applying the “clear and present danger” test to defendant’s speech).
\(^{83}\) Id. at 104 (citing GEORGE B. TRUBOW, PRIVACY LAW AND PRACTICE (1991)).
Autonomy is the ability of an individual to engage in private activities free from intervention or regulation. Autonomy allows people to make decisions freely and act as individuals.

Privacy also includes an interest against intrusion. It "means being free from surveillance in situations in which an individual has a reasonable expectation of privacy." The argument against intrusion is tied to the anonymity of individuals. Anonymity in this context does not signify a complete lack of ability to identify someone; rather, it refers to an individual's ability to go about his or her daily life without someone watching every move. Surveillance technology is designed to intrude upon this anonymity and, in certain situations, society accepts this intrusion. It is unclear what types of intrusion and to what extent intrusion is acceptable when new advances in surveillance are involved.

The third aspect of privacy is information or data privacy. Information privacy is also tied to the concept of anonymity. Instead of addressing an individual's actions and movements, it is concerned with the individual's personal information. Individual bits of personal information can identify a person and his or her activities. When various items of personal information are pieced together, an even more telling picture can develop. The argument for information privacy stems from the concern that individuals have a right to some control over who has access to their personal information and for what purpose.

New technology can encroach upon all three privacy interests. Intrusion and information privacy interests, however, are particularly affected by the technologies and their merger as discussed here.

As Sheri Alpert points out, these three interests in privacy are "by no means mutually exclusive." For the benefit of discussion of the right of privacy, however, it is helpful to separate them into distinct categories.

84. Id. at 104.
85. Although an autonomy interest is important to the concept of privacy, neither surveillance technology nor personal information problems disturb the autonomy aspect of privacy.
86. Alpert, supra note 82, at 105.
87. Id.
88. Steven A. Bercu, Toward Universal Surveillance in an Information Age Economy: Can We Handle Treasury's New Police Technology?, 34 JURIMETRICS J. 383, 400 n.89 (1994).
89. This concern arises out of anonymity concerns in the same way as the interest against intrusion does. Information privacy concerns differ from intrusion concerns, however, in that they address an individual's personal information, rather than the individual himself.
C. Surveillance Intrusion, Wiretapping, and the Fourth Amendment

There is no specific constitutional right to privacy. The Supreme Court, however, developed a limited right of privacy based on a jurisprudence of "fundamental rights" in a string of cases—Griswold v. Connecticut,90 Roe v. Wade,91 Whalen v. Roe,92 and Bowers v. Hardwick.93 The Supreme Court has described this right as a "penumbral right," flowing from the emanations of the First, Third, Fourth, Fifth, Ninth, and Fourteenth Amendments.94 It generally has been limited to certain rights of privacy and autonomy in individuals' intimate life decisions, such as whether to have children or to engage in consensual sexual intercourse while married.95

1. Search Warrants

Surveillance activity directly relates to an individual's interest against intrusion because it is an intentional attempt to observe that which the individual believes to be private. The discussion of the relationship between surveillance activity and privacy concerns begins with the Fourth Amendment of the Constitution.96 An unconstitutional search is an unreasonable intrusion on an individual's privacy rights.97 The placement of surveillance devices on a subject's private property by law enforcement agencies requires a search warrant issued by a court.98 For example, courts generally express a willingness to approve both audio and video surveillance, provided that the type of crime necessitates it and the surveillance does not involve the observance of purely private activities. New developments in surveillance technology, however, can further

90. 381 U.S. 479 (1965).
94. Burrows, supra note 10, at 1090-91; Griswold, 381 U.S. at 484-85.
95. Burrows, supra note 10, at 1091-2003. "In Griswold v. Connecticut, the court changed the field of privacy...sparking a new type of privacy that resulted from a combination of technological advances in birth control and the personal choice to exercise privacy rights in this area." Id. at 1091.
96. U.S. CONST. amend. IV. It is the search aspect of the Fourth Amendment to which surveillance activity relates.
97. See, e.g., Katz v. United States, 389 U.S. 347, 350 (1967) (holding that the Fourth Amendment "protects individual privacy against certain kinds of governmental intrusion").
complicate the question of what constitutes such a search. Courts have not yet been presented with the question of the use of facial recognition technology in connection with video surveillance.

In early Fourth Amendment jurisprudence, the Supreme Court used the trespass doctrine to determine whether governmental activities amounted to an unconstitutional search. The Court used what was termed an “area-based” approach and narrowly construed the Fourth Amendment. It held that a search did not occur unless physical intrusion into one of the subject’s “constitutionally protected areas” occurred. Surveillance such as wiretapping, which did not require physical intrusion, did not constitute a search, and thus, did not require a warrant.

In 1967, the Supreme Court replaced the trespass doctrine with the Katz doctrine. In Katz v. United States, the Court found that a telephone wiretap constituted a search. The decision extended Fourth Amendment protection by reasoning that “the Fourth Amendment protects people, not places.” The Court in Katz found that surveillance technology could violate an individual’s interest against intrusion even without any physical trespass.

The Katz doctrine has been used to determine whether a search has occurred. The test from Katz, as articulated in Justice Harlan’s concurring opinion, consists of two prongs that examine subjective and objective factors. Under the first prong of the test, the subject

---

100. The Court established the trespass doctrine in Olmstead v. United States, 277 U.S. 438, 465 (1928) (holding that a wiretap did not constitute an illegal search because no physical intrusion of the defendant’s “houses, persons, papers, and effects” occurred).
103. Olmstead, 277 U.S. at 466.
105. Id. at 351.
106. Id. at 362 (Harlan, J., concurring) (holding that Fourth Amendment protections extend beyond physical invasion, because “in the present day... reasonable expectations of privacy may be defeated by electronic as well as physical invasion”).
107. Id. at 360-62 (Harlan, J., concurring).
must "have exhibited an actual (subjective) expectation of privacy." The second prong then assesses whether that "expectation [is] one that society is prepared to recognize as 'reasonable.'" For activity, including surveillance, to constitute a search under Katz, both prongs of the test must be met. The Katz test as applied by many courts, however, does not provide sufficient protection against numerous emerging technologies.

Federal courts apply the standards handed down by the Supreme Court in audio surveillance cases when reviewing the legitimacy of video surveillance orders. In United States v. Torres, the Seventh Circuit upheld the use of video surveillance, balancing the necessity of the surveillance against the level of intrusion (i.e. the type of crime involved weighed against the premises where the video surveillance was used). The government obtained an order allowing the placement of video surveillance in a "safe house" of an organization suspected of terrorist activities. The court concluded that the order allowing the video surveillance was proper because private activities were not involved and the activities were of an illegal nature. The court explained, however, that video surveillance represents an extremely intrusive form of technology and the constitutional standard for issuing a warrant should be high. The court borrowed

108. Id. at 361 (Harlan, J., concurring).
109. Id.
110. See United States v. Torres, 751 F.2d 875, 880-81 (7th Cir. 1984). To date, federal appellate courts have decided only three cases involving video surveillance. See id. at 875; United States v. Biasucci, 786 F.2d 504 (2d Cir. 1986); United States v. Cuevas-Sanchez, 821 F.2d 248 (5th Cir. 1987).
111. 751 F.2d at 882. The court did state that "television surveillance is exceedingly intrusive... and inherently indiscriminate, and... could be grossly abused - to eliminate personal privacy as understood in modern Western nations." Id.
112. Id. at 877. The defendants were members of Fuerzas Armadas de Liberacion Nacional Puertorriquena (FALN), a group that wanted the territory of Puerto Rico to separate from the United States. Id. at 876. The FALN was responsible for a number of bombings in New York, Chicago, and Washington D.C. Id. Using video surveillance, the government watched as some of the defendants assembled the bombs. Id. at 877.
113. Id. at 883. "[T]he invasion of privacy caused by secretly televising the interior of business premises is less than that caused by secretly televising the interior of a home, while the social benefit of the invasion is greater when the organization under investigation runs a bomb factory than it would be if it ran a chop shop or a numbers parlor." Id.
114. Id. at 883-84. The court noted that even video surveillance conducted pursuant to a warrant could be held unconstitutional if the intrusiveness of the search
provisions of Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III) that implemented the Fourth Amendment’s requirements of particularity in warrants.

In United States v. Biasucci, the Second Circuit also followed Title III as a guide to Fourth Amendment analysis. The government charged the defendants with violating the Racketeer Influenced and Corrupt Organization Act. During the government’s investigation, the court granted an order authorizing video surveillance inside the defendants’ place of business. “Finding the reasoning of Torres to be compelling,” the court held “district courts, federal magistrates, and state judges may authorize television surveillance of private premises in appropriate circumstances.” However, the court failed to explain why video surveillance was necessary under the circumstances.

United States v. Cuevas-Sanchez is a more recent federal appellate decision involving video surveillance. In Cuevas-Sanchez, the government obtained a warrant allowing video surveillance of the exterior of an alleged drug dealer’s home. The government placed exceeded the necessity of using video surveillance. Id. at 883.


116. Torres, 751 F.2d at 885. The Title III provisions were the particularity of the search, 18 U.S.C. § 2518(1)(b) (1994), the necessity of using video surveillance, 18 U.S.C. § 2518(1)(c) (1994), and the time period in which the surveillance is to occur, 18 U.S.C. § 2518(1)(d) (1994).


118. Biasucci, 786 F.2d at 506; see Racketeer Influenced and Corrupt Organization Act, 18 U.S.C. §§ 1961-1968 (1982). The defendants were appealing the trial court’s decision to admit videotapes recorded by surreptitious surveillance that had been installed pursuant to a warrant issued by a district court. Biasucci, 786 F.2d at 506.

119. Biasucci, 786 F.2d at 507.

120. Id. at 509.

121. Denise Troy, Comment, Video Surveillance Big Brother May Be Watching You, 21 ARIZ. ST. L. J. 445, 453 (1989) (highlighting the Title III principles covering audio surveillance that federal courts have borrowed in the absence of express legislation on video surveillance). Unlike Torres where video surveillance was necessary because the terrorists acted in silence, Biasucci does not explain why the government needed to use video surveillance in addition to other forms of electronic surveillance. Id. at 453.

122. 821 F.2d 248 (5th Cir. 1987).

123. Id. at 249-50.
the video camera on a utility pole overlooking a tall fence at the back of the defendant's property. The Fifth Circuit rejected the government's argument that the defendants could not have had a reasonable expectation of privacy in their backyard because it could be seen from a variety of different locations. The court invoked principles from Title III, believing, as the Torres and Biasucci courts did, that doing so would safeguard the defendant's Fourth Amendment rights sufficiently. The majority felt the warrant satisfied the statutory requirements, and concluded that the Fourth Amendment had been satisfied.

In Cuevas-Sanchez, the Fifth Circuit adopted the standard from Torres but applied it less strictly, concluding that the video surveillance was not absolutely necessary but approving it anyway. Neither Cuevas-Sanchez nor Biasucci appears to have balanced the necessity of the video surveillance against its level of intrusiveness.

2. Exceptions to the Warrant Requirement

The plain view doctrine is an exception to the warrant requirement. If something illegal is in plain view, there is no need for a warrant because law enforcement officials did not have to search to find it. Thus an officer has the right to seize illegal property in plain view without a warrant. Originally, the plain view exception required that police discover the evidence inadvertently. In Horton v. California, however, the Supreme Court eliminated the inadvertence requirement for a plain view seizure.

124. Id. at 250.
125. Id. at 250-51.
126. Id. at 251-52.
127. Id. at 252.
128. Troy, supra note 121, at 456. The crime under surveillance was not life threatening and occurred in the back yard of Cuevas-Sanchez' home. The court recognized that a camera was not necessary to obtain the information sought. Nevertheless, the court still upheld the warrant.
129. Id. The courts did not appear to be balancing the type of crime involved with the place to be searched, and so would appear to be relaxing the standards for video surveillance warrants.
133. Id. at 137-42.
Another exception to the warrant requirement is the open fields doctrine. The doctrine suggests that if an item cannot be classified as a person, house, paper, or effect, the item is not entitled to Fourth Amendment protection against search or seizure. This is particularly true where the owner has not taken reasonable precautions to ensure privacy. The open fields doctrine arises in cases involving warrantless aerial surveillance by law enforcement agencies.

3. Information Privacy

Information privacy is based on an autonomist view of individuals. Personal data is part of the "self." The autonomist view construes the right to privacy as protecting the information that comprises a person's "data image." As society becomes more information-based, the need for individuals to distribute their personal information increases. An unwillingness to give personal information to others effectively prevents an individual from fully functioning in society. As personal information becomes more important and is accessible to a greater number of people and institutions, the need to protect such private information intensifies.

Although the Fourth Amendment addresses the tension between the interest against intrusion and surveillance technology, no constitutional clause addresses the specific right to privacy. The regulation of information privacy, however, still begins with the

134. Id.
135. Id. The Fourth Amendment specifically discusses "the right of the people to be secure in their persons, houses, papers, and effects ..." U.S. CONST. amend. IV. "However reasonable a landowner's expectations of privacy may be, those expectations cannot convert a field into a 'house' or an 'effect.'" Oliver v. United States, 466 U.S. 170, 184 (1984) (White, J., concurring). See also Granholm, supra note 130, at 693.
136. Granholm, supra note 130, at 693.
137. Id.
138. Bercu, supra note 88, at 401. See also ELLEN ALDERMAN & CAROLINE KENNEDY, THE RIGHT TO PRIVACY 326 (1995) ("A portrait of you ... will exist in cyberspace. The profile could be so complete that it will be like having another self living in a parallel dimension; it is a self you cannot see, but one that affects your life just the same.").
139. Id.
Because no right to privacy is enumerated in the Constitution, there is disagreement over what the right entails. Statutes that regulate information privacy generally regulate governmental use of personal data more broadly and strictly than private use of such data.

The Supreme Court has examined the issue of information privacy only once. In *Whalen v. Roe,* the Court held that the State of New York could maintain a database of individuals who legally obtained narcotics by prescription. The Court found that the legitimate state interest in regulating prescription drugs outweighed the individual's privacy right in the personal information contained in the database. In dicta, however, the Court explicitly recognized that an information privacy interest exists.

Just as the right to reproductive privacy established in *Griswold* remained uncertain until subsequent decisions by the Court, the right to information privacy similarly remains unclear. Scholars generally agree that, at present, the right to privacy in personal information is weak. However, as personal information begins to play a greater role in individuals' daily lives and the interest in personal information privacy increases, the need to develop this right will increase as well.

**D. Federal Statutory Enactments**

On the federal level, Congress has not yet enacted legislation to protect individuals from the widespread use of video surveillance, facial recognition, or other new surveillance technologies. Courts, however, use Title III and the Privacy Act of 1974 to prevent abuses of these technologies.

---

143. Id.
145. Id. at 591.
146. Id. at 598-602.
147. Id. at 605 (“The right to collect and use such data for public purposes is typically accompanied by a concomitant... duty to avoid unwarranted disclosures... In some circumstances that duty arguably has its roots in the Constitution...”).
149. Burrows, *supra* note 10, at 1083. “Congress has never directly addressed the use of video surveillance on public streets.” Id.
151. See generally Troy, *supra* note 121, at 448-49 (discussing traditional Fourth
Privacy Rights in the United States and the United Kingdom

Title III restricts aural surveillance (wire and phone taps) where none of the parties to the conversation consented. It does not specifically address or encompass video surveillance. Before law enforcement can use audio surveillance (and video surveillance by analogy), Title III requires: (1) probable cause, (2) particularity (type of crime, location, type of communication, and identity of surveillance subject), (3) necessity (must be able to show that other more traditional and less intrusive forms of surveillance cannot succeed), and (4) minimization (must minimize the interception of non-relevant conversation and activity). In 1986, Congress amended Title III to correspond with the good faith exception to the exclusionary rule.

The Privacy Act of 1974 restricts the collection, use, and dissemination of personal information by federal agencies and allows individuals the right to access and correct such information. The Act also controls the matching of information from several government databases, commonly referred to as “data creep.” The law prohibits federal employees from disclosing any data that could incorporate an individual’s biometric signature to any party not entitled to receive that information. Federal employees are not prohibited from releasing the information to other federal agencies or to federal or state law enforcement agencies.

E. State Privacy Protections

States have the power to create rights for their citizens, beyond those protected by the U.S. Constitution. Proposals to regulate or

Amendment requirements).
152. Id. at 445.
153. Id. at 448.
155. 18 U.S.C. § 2518(10)(c) (Supp. 1986). The good faith exception was announced in United States v. Leon, 468 U.S. 897 (1984). If a law enforcement officer has a good faith belief that a warrant is valid, then evidence found pursuant to the warrant is not excludable. Id. at 919-20.
157. This statute prohibits disclosure of personal information “without the written consent of an individual to whom the record pertains unless the disclosure is for the purpose for which the data was collected.” Petti, supra note 45, at 732.
160. Id. The head of the federal agency or law enforcement agency must formally request the portion of the record desired and describe the purpose for which it is desired. Id.
terminate law enforcement’s ability to use video surveillance may find support in state privacy rights as expressed in state constitutions or statutes. Some states, including Oregon, Pennsylvania, Alaska, Hawaii, and Montana, explicitly articulate an individual right to privacy in their state constitutions. Many civil liberties and criminal defense lawyers count on state courts, which are often more protective of individual rights than federal courts, to check the use of new surveillance technologies.

The California Constitution specifically includes privacy as an inalienable right. In many of its rulings, the California Supreme Court has indicated that the scope of the protection granted by the state constitution’s explicitly enumerated privacy right is at times greater than the scope of the U.S. Constitution’s unenumerated right of privacy. In the context of privacy claims by defendants in criminal trials, however, the California Supreme Court has held that the right to privacy guaranteed by article 1, section 1 of the California Constitution is merely coextensive with the federal right guaranteed by the Fourth Amendment. With respect to surveillance in the search and seizure context, the privacy protections of the California Constitution currently apply only where the parties to the conversation have a reasonable expectation of privacy in what is said. Thus, although the California Constitution’s explicit articulation of an individual right to privacy could allow courts to check law enforcement’s use of powerful new surveillance technologies, it has yet to be used that way.

---

162. Id. State courts must have adequate and independent grounds for decisions resting on state constitutional rights and must make a plain statement that, in the court’s judgment, the case was decided on state constitutional law. Id. at 1112.

163. Id. at 1113-14. Montana employs a strict scrutiny test in cases involving privacy rights. Id.

164. Hansen, supra note 17, at 48.

165. CAL. CONST. art. I, § 1. (“All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.”)

166. See, e.g., Santa Barbara v. Adamson, 610 P.2d 436, 440 n.3 (Cal. 1980) (noting that the federal right to privacy “appears to be narrower than what the voters approved in 1972 when they added ‘privacy’ to the California Constitution”).


169. See generally J. Clark Kelso, California’s Constitutional Right to Privacy, 19 PEPP. L. REV. 327 (1992) (noting that the California Constitution explicitly declares that state constitutional rights are independent of corresponding federal
F. American Bar Association Proposed Standards

The American Bar Association (ABA) has proposed standards with respect to "technologically assisted physical surveillance." These standards expand on the uses of video surveillance by permitting its use for the interception of private communications (wiretapping). The standards support use of facial recognition technology when "it is reasonably likely to achieve a legitimate law enforcement objective, approved by a politically accountable political official, and presented to the public with an opportunity for comment." Where video surveillance is used for deterrence purposes, the ABA believes the public must first be notified of the proposed video camera and allowed to express its views. While having no binding legal effect, the ABA's standards constitute persuasive authority and encourage public debate over the use of video surveillance.

G. Current Effect of U.S. Privacy Rights on Video Surveillance and Facial Recognition Technology

Facial recognition technology is most likely to be used as part of a law enforcement video surveillance system monitoring public areas such as airport terminals, border entry points, and housing projects. Currently, it is unlikely the Supreme Court would characterize public video surveillance by law enforcement agencies as a "search" within the meaning of the Fourth Amendment, as the Court has said there is no reasonable expectation of privacy in public areas.

Under the Katz test, a court considers whether the individual reasonably expects to be free of surveillance in the areas where he or she is carrying out activities. While in public, most people generally expect to be observed by others, such as being monitored or videotaped while in a convenience store or in the office building in constitutional rights).

171. Slobogin, supra note 170, at 440.
172. Hansen, supra note 17, at 48.
173. Ward, supra note 26, at S8.
which they work. On the other hand, most people expect to be free from surveillance in the home.

Under the plain view doctrine,\footnote{See supra pt. III(C)(2).} information discovered through the use of video surveillance and facial recognition technology would generally not violate privacy rights. Discovery of illegal acts with the technology is analogous to discovery of information in the plain view of law enforcement officials. Particularly because of the elimination of the inadvertence requirement, it is likely that video surveillance and facial recognition technology could be validated under the plain view doctrine.

Under the open fields doctrine,\footnote{See supra pt. III(C)(3).} the use of facial recognition technology to extract a facial signature from a video image would be considered far less intrusive than extraction of biological samples from a person’s body. The Supreme Court, however, generally considers the gathering of individuals’ physiological or biometric information by the government as a “search” under the Fourth Amendment.\footnote{Petti, supra note 45, at 723.}

Under the Torres test, courts consider the level of intrusiveness of facial recognition technology and video surveillance.\footnote{See United States v. Torres, 751 F.2d 875 (7th Cir. 1984).} Because facial recognition technology is the least intrusive method available, it is likely that a court would find that this technology passes the Torres test.\footnote{Id. at 883. While it is unknown whether the Supreme Court would consider the use of facial recognition technology to gather biometric signatures as an unreasonable invasion of privacy, the Court has allowed the government to violate a person’s reasonable expectation of privacy when it advances a legitimate government interest.}

Whether a constitutional “right to privacy” will stymie efforts to implement facial recognition technology and video surveillance depends on the extent and uses of these surveillance systems.\footnote{Petti, supra note 45, at 726. This presumably includes the corresponding public perception and response to the program.} If facial recognition technology or some other biometric identifier becomes too pervasive, federal and state courts might fight to invalidate the technology out of fear that the federal government was trying to track every move of each citizen.\footnote{Id.} The social security
number, however, is now used as a de facto national identification device and no court has invalidated its use.183

IV. The Right to Privacy in the United Kingdom

A. History

Although the right to privacy originated in the United States, the first data privacy legislation was passed in Europe in 1970.184 The European interest in personal privacy is rooted in recent history, stemming largely from its experience in population control exercised by Nazi Germany during World War II.185

The modern right to privacy is asserted in Article 8 of the European Convention on Human Rights (ECHR).186 Article 8, which was incorporated into U.K. law by the Human Rights Act of 1998, binds states to respect individual privacy.187 Article 8, and now the Human Rights Act of 1998, assert that interference with privacy is permissible only when it is necessary and carried out in accordance with the law.188 The Human Rights Act of 1998 voided the common law approach, which had allowed the police to do whatever they wanted as long as it was not prohibited by law.

In July 2000, the Data Protection Commissioner (DPC) published the Data Protection Act 1998 (DPA), setting out for the first time a comprehensive legal framework for the use of CCTV systems.189 The Regulation of the Investigatory Powers Act 2000 also became relevant to issues of privacy and surveillance.190

183. Id. at 727. The government does not yet have the ability to track every individual's movements with his or her social security number. "Today, private enterprises and universities along with the government use the social security number as identification." Id.
185. Id.
187. Id.
190. Ward, supra note 186.
B. Article 8 of the European Convention on Human Rights

The Human Rights Act of 1998 came into full effect on October 2, 2000. It incorporated into domestic U.K. law most of the rights contained in the ECHR. This included Article 8 of the ECHR. Article 8 states "[e]veryone has the right to respect for his private and family life, his home and his correspondence," and allows interference with this right by the state only where it is necessary for certain purposes. In the context of the collection of evidence in criminal matters, these purposes include the interests of national security and public safety, and the prevention of disorder or crime. In accordance with the principles established in Sunday Times v. United Kingdom, the law must prescribe any interference, and the interference must have a legal basis which is accessible and precise enough to enable people to know when interference is allowed. In addition, the interference must be necessary and proportionate in the context of criminal evidence. Relevant questions include whether the method of surveillance is the least intrusive, whether other methods have been tried and found ineffective, and whether the offense is of sufficient gravity to justify surveillance and the resulting breach of privacy. A system of accountability must exist, preferably independent of the police, to authorize and monitor the use of surveillance. Where the use of surveillance aggrieves a person, a means of determining whether privacy rights have been violated and mechanisms to provide a remedy must exist.

192. Id.
194. Id. art. 8(2).
195. Id.
197. Id.
198. Id.
200. Id.
C. The Data Protection Act 1998

The DPA regulates the use of “personal data.”201 It went into effect on March 1, 2000, implementing the European Community Directive202 on the protection of individuals with regard to the processing of personal data and the free movement of such data (EC Directive).203

1. Definitions

The EC Directive is clear that “techniques used to capture, transmit, manipulate, record, store or communicate sound and image data relating to natural persons” are included in the DPA.204 The EC Directive is realized in the DPA definitions.205 The DPA defines “personal data” as “data which relate to a living individual who can be identified either from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller ...”206 This definition is not limited to circumstances where a data controller can attribute a name to a particular image.207 The DPA definitions cover any image of an individual’s features from which that individual could be identified.208 The DPA defines “processing” of personal data extremely broadly, covering all sorts of recording and holding of images (even if just for a limited period of time or if no further reference is made to those images) as well as real-time transmission of the images or any further use or disclosure.209

Based on the DPA definitions, it is clear that the DPA covers video surveillance and the use of facial recognition technology. Further, where the data is “sensitive,” more stringent conditions apply.210 Sensitive data includes information regarding the commission or alleged commission of an offence.211

CCTV surveillance is undertaken for various purposes, and the

201. Wadham, supra note 189.
203. Wadham, supra note 189.
204. Id.
205. Data Protection Act 1998, c. 29, § 1 (Eng.) [hereinafter DPA].
206. Id. § 1(1).
207. Wadham, supra note 189.
208. Id.
209. See DPA, supra note 205, § 1(1).
210. Wadham, supra note 189.
211. Id.
The legal framework differs according to those purposes. Broadly, these purposes can be categorized as: (1) directed covert surveillance, (2) intrusive covert surveillance, (3) other covert surveillance, and (4) non-covert surveillance. The DPA covers all these purposes. In addition, the first two categories are subject to the specific provisions of the Regulation of Investigatory Powers Act. Therefore, the only form of CCTV surveillance that the statute regulates is when an individual carries out CCTV for the purpose of "personal, family, or household affairs."

2. Principles

The DPA sets out eight principles with which data controllers must comply. While all eight principles are binding, this Note discusses only those that are relevant to CCTV. The first principle is fair and lawful processing. Fair and lawful processing requires adherence to the conditions set out in the DPA. It also requires that certain information be provided or made readily available to the individual, including the identity of the data controller and the general purpose for which the data is being processed. When determining fairness, courts look to the method that the police used to obtain the data. Processing is not fair if the individuals are deceived or misled as to the purpose for which the data is collected and processed. Posting appropriate signs might satisfy both elements. Clearly, a posting is not possible for covert surveillance. However, the DPA provides an exemption where the purpose of surveillance is prevention and detection of crime or apprehension and prosecution of offenders. The requirement for lawful processing means that other statutory or common law restrictions must be taken

212. Id.
213. Id.
214. Id.
215. Id.
216. DPA, supra note 205, § 36.
217. Wadham, supra note 189.
218. Id.
220. Wadham, supra note 189.
221. Id.
222. Id.
223. Id.
into account. For example, where the information is confidential, the common law duty of confidentiality has to be complied with in addition to the specific provisions of the DPA.

The second principle with which data controllers must comply is that the data may be obtained only for one or more specified and lawful purposes and may not be further processed in any manner incompatible with that purpose. This principle means a data controller must be clear about the purpose(s) for which the images are processed and, if disclosure is to be made to a third party, the data controller must consider the purposes for which the third party might process the data in order to ensure compatibility.

The third principle requires that data be adequate, relevant and not excessive in relation to the purposes for which it is processed. For example, cameras installed for the purpose of recording acts of vandalism in a parking lot should not overlook neighboring private residences, and blurred images may be inadequate because they have no evidential value.

The fifth and final principle relating to CCTV requires that data not be held any longer than necessary for the purpose for which it is processed. It may therefore be necessary to destroy data, for example, after all legal proceedings have terminated.

3. Rights of Data Subjects

The DPA accords data subjects particular rights. The DPA allows a data subject the “right to be informed when the controller is processing their personal data, the right to object to processing, and the right to have the controller rectify incorrect personal data.” The DPA also gives the data subject the right to prevent processing for direct marketing, and the right to require that no decision that significantly affects the data subject be made solely by automated means where it is to be used to evaluate matters relating to him (e.g.

---

224. Id.
225. DPA, supra note 205, § 4(1) of 2, sched. 1, pt. I.
226. Wadham, supra note 189.
227. DPA, supra note 205, § 4(1) of 2, sched. 1, pt. I.
228. DPA, supra note 205, § 4(1) of 2, sched. 2, pt. I.
229. Wadham, supra note 189.
231. Id.
performance at work). Finally, the data subject has the right to require rectification, blocking, and destruction or erasure of inaccurate data by application to the court.

4. Exemptions and Remedies

Specific exemptions that may be relevant to CCTV include the following purposes: processing for prevention or detection of crime; apprehension or prosecution of offenders; safeguarding national security; certain regulatory activities; journalism, literature or art; and disclosures required by law or made in connection with legal proceedings.

Where a breach of the DPA occurs, the individual can either go to the courts or make a claim to the DPC. If satisfied that a breach has occurred, the DPC can serve an enforcement notice on the data controller, requiring the person to refrain from processing or to process only in a way that does not infringe on the individual's rights. If the individual can prove actual damage, he or she can receive compensation. Failure to comply with a notice is punishable by a fine.

Recently, the use of CCTV was challenged in the domestic courts in R. v. Brentwood Borough Council, ex parte Peck. The case is now pending before the European Court of Human Rights. There is an issue as to whether privacy applies at all to the recording of images which are within public space, but this is assumed for the purposes of the DPA and is clearly a matter of fact in any particular case.


The controversial Regulation of Investigatory Powers Act 2000 (RIP Act) entered Report Stage in the House of Lords on July 10,
2000 and received Royal Assent on July 28, 2000. The stated purpose of the RIP Act is to ensure that investigatory powers are used in accordance with human rights. To achieve this end, the RIP Act sets out the purposes for which such powers may be used, which authorities may use them, who may authorize use, what use may be made of material gained, independent judicial oversight, and a means of redress for the individual. The RIP Act includes "arrangements for updating and expanding the law governing the interception of communications, the acquisition of data relating to communications and the regulation of surveillance activities" to ensure they are in compliance with the European Union Telecommunications Data Protection Directive and the ECHR. It purports to close the loophole in U.K. law unearthed in Halford v. United Kingdom. The RIP Act extends the general prohibition on interception to private as well as public telecommunications systems. It also regulates the interception of e-mail and decryption of collected material. The RIP Act also statutorily authorizes the use of covert surveillance by the security and intelligence agencies, law enforcement, and other public authorities.

The RIP Act provides that any conduct carried out in accordance with an authorization will be lawful (whether that conduct is in the United Kingdom or abroad). In addition, if neither this Bill nor existing legislation requires separate authorization, incidental conduct will not be subject to civil liability.

The RIP Act covers two types of covert surveillance: directed surveillance and intrusive surveillance. Directed surveillance is surveillance undertaken in relation to a specific investigation or a specific operation which is likely to result in the obtaining of private

---

241. Ward, supra note 186; Voutourides, supra note 191; see Regulation of Investigatory Powers Bill 2000, cl. 26 (Eng.) [hereinafter RIP Act].
242. Wadham, supra note 234.
243. Id.
244. Voutourides, supra note 191.
245. Ward, supra note 186.
246. Id.
247. Id.
248. Wadham, supra note 234. Covert surveillance is surveillance carried out such that the subject of the surveillance is unaware that it is taking place. RIP Act, supra note 241, cl. 26(9).
249. RIP Act, supra note 241, cl. 27.
250. Wadham, supra note 234.
251. Id.
information about a person and not done as an immediate response to events or circumstances that would make it impracticable to seek an authorization. Authorization can be granted only where the person authorizing the surveillance believes that it is (1) in the interests of national security; (2) for the purposes of preventing or detecting crime or preventing disorder; (3) in the interests of the economic well-being of the United Kingdom; (4) in the interests of public safety; (5) for the purpose of protecting public health; (6) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department; or (7) for other purposes which may be specified by order of the Secretary of State. Authorization can also be granted where the authorized activity is proportionate to what it seeks to achieve. Only the Secretary of State has the authority to prohibit certain conduct or impose additional requirements for authorization on certain types of directed surveillance.

Intrusive surveillance is surveillance carried out in relation to anything taking place on residential premises or in any private vehicle. Surveillance devices that only provide information about the location of a vehicle, for example, are not covered. Only the Secretary of State and senior officers can authorize intrusive surveillance, and such surveillance may be authorized only if it is “(1) in the interests of national security, (2) for the purpose of preventing or detecting serious crime, (3) in the interests of the economic well-being of the U.K., or (4) where the authorized activity is proportionate to what it seeks to achieve.” The authorizing officer then must determine whether the information could be obtained through less intrusive means.

The government’s stated intention in promoting the RIP Act is to “put beyond doubt the legality, in human rights terms, of intrusive surveillance of the kind addressed by the Act.” However, this
system of authorization is not mandatory. Failure to comply merely results in official sanction. Fortunately, the DPA still applies in cases where no authorization is sought or given, and where the surveillance does not fall within the RIP Act. As already noted, the DPA implements the EC Directive and the EC Directive refers specifically to Article 8 of the ECHR. Scholars observe that the EC Directive expressly requires member states to “protect the fundamental rights and freedoms of natural persons, in particular their right to privacy, with respect to the processing of personal data.” Nevertheless, Article 8 of the ECHR should be considered an additional requirement, above and beyond the DPA and the RIP Act’s consideration of the “in accordance with the law” prong of Article 8.

Where surveillance is secret, it undeniably interferes with an individual’s right to private life. Under Article 8(2), however, the legitimate uses of government surveillance include (1) national security, (2) public safety, (3) the economic well-being of the country, (4) prevention of disorder or crime, and (5) protection of the rights and freedoms of others. The more difficult issue will be deciding whether in a particular case the surveillance was “necessary in a democratic society.” This will depend upon whether, on the facts of the case, the means used are proportionate to the aim being pursued. In terms of Article 8, this means that there must be a pressing social need for the interference, not merely a good reason for it. The aim is to achieve a fair balance between the general interests of the community and the need to protect individuals’ rights.

261. Id.
262. Id.
263. Id.
264. Id.
265. Id.
267. European Convention on Human Rights, supra note 193, art. 8(2).
268. Wadham, supra note 234.
269. Id.
270. Id.
271. Id.
E. Current Effect of U.K. Privacy Law Video Surveillance and Facial Recognition Technology

Facial recognition technology and video surveillance is legal in the United Kingdom, and has in fact been extensively used there for the past few years. The United Kingdom, years ahead of the United States in dealing with public video surveillance and facial recognition technology, is now addressing the effects of new technology on privacy rights by enacting new laws regulating its use. These new U.K. regulations can serve as an example from which the United States can build upon and learn from in the near future.

V. Proposed Regulation: Learning from U.K. Regulations on Video Surveillance and Facial Recognition Technology

In dealing with the impact of video surveillance and facial recognition technology, the United States could learn from the recently enacted U.K. regulations. The entire area of law pertaining to privacy rights in the United States and its invasion by new technology is inadequate. Rather than waiting for the courts to try to catch up with the technology, the United States should follow the United Kingdom’s lead by enacting new regulations and laws dealing with emerging technology.

A. Likelihood of New Laws Regulating Privacy Rights

The European approach to privacy rights, however, differs from that of the United States, and these differences are likely to prevent implementation of entirely new regulations in the United States. European nations take an omnibus approach to individual rights and give the state a proactive preventive role. The European emphasis is on the deterrence of harm, which is accomplished by instituting control mechanisms necessary for oversight.

In contrast, the United States patches together provisions of the U.S. Constitution, state constitutions, federal and state legislation, and state common law to address the right to privacy. It takes a reactive approach by legislating in narrow specific areas where problems have occurred. This approach emphasizes use of

272. Heydrich, supra note 184, at 412.
273. Id.
274. Id.
275. Id.
remedies for damage that has already taken place and prevents future harm via threat of legal action.\textsuperscript{26}

Therefore, because of this patchwork method of privacy regulation, the United States may never have an over-arching privacy statute. However, a clearer federal privacy protection policy is necessary for the United States to provide adequate protections for the right to privacy in the face of emerging technologies.\textsuperscript{27}

\textbf{B. Proposed Regulation}

Proposed regulation could be incorporated on either a federal or state level based on the \textit{Torres} test.\textsuperscript{28} For the use of video surveillance, the regulation should balance the necessity of the surveillance against the level of intrusion to establish a clear rule for what type of video surveillance is allowed. The proposed regulation would recognize the benefits of decreased crime in areas that have implemented video surveillance and use of facial recognition software.

In the interests of promoting the use of technology to aid law enforcement, surveillance in any place that is not a private dwelling or other obviously private area, e.g. restrooms or changing rooms, should be considered low intrusion when used for law enforcement purposes. Expectations of privacy are generally lower in public places. Therefore, surveillance in these areas would not chill human behavior and interaction.\textsuperscript{29} Human behavior naturally adjusts merely by being in public areas. However, in order to put the public on notice, the government should post signs in areas where non-covert video surveillance occurs.

The rule would permit all surveillance conducted by law enforcement or government agencies for: (1) national security; (2) public safety; (3) the economic well-being of the country; (4) prevention of disorder or crime; or (5) protection of the rights and freedoms of others. The rule would require all other surveillance interests, including private individuals who wish to conduct video surveillance in public, to apply to the appropriate government agency and detail the necessity of surveillance versus the level of intrusion.

\textsuperscript{26} Id.
\textsuperscript{27} Fromholz, \textit{supra} note 142, at 483.
\textsuperscript{28} United States v. Torres, 751 F.2d 875 (7th Cir. 1984).
This rule would enable the use of video surveillance only when necessary for the public good. For covert surveillance, the regulation should be stricter. All covert surveillance would require filing and authorization before being permitted.

Some commentators fear that the use of facial recognition surveillance technology will lead to discriminatory targeting of certain groups. In order to avoid discriminatory profiling, monitors would have to follow a preset scanning pattern of the vicinity, thereby eliminating any biased surveillance. Human intervention in the surveillance would only be allowed in the case where a match was made. When video surveillance is used in conjunction with facial recognition technology, images collected that do not match the criminals listed in a database must be discarded immediately. No surveillance images would be retained unless a match was found. Therefore, most people would not have to fear that a romantic rendezvous in the park would be captured indefinitely on film.

Moreover, personal information, including biometric and commercial information, should not be released to private individuals. This compilation of data should be allowed for law enforcement and related purposes only. Furthermore, a watchdog agency other than the overcrowded courts should be set up to monitor government collection and use of video surveillance data.

VI. Conclusion

The use of video surveillance and facial recognition technology is justified for law enforcement purposes when properly limited to use only in public areas where there is little or no expectation of privacy. Particularly in the aftermath of the September 11 terrorist attacks, surveillance measures utilizing new technologies will increase. The current law in the United States draws a fuzzy line between valid and illegal surveillance and fails to address the privacy concerns arising from the use of new technologies. Proper regulation that balances the right to privacy and the need for efficient law enforcement would allow individuals' personal autonomy to thrive in a much safer environment.

The United States is still searching for answers to the issues arising from the use of new technologies; until the United States enacts comprehensive legislation, it will continue to merely react to

280. Id. at 328.
technological invasions of privacy rights or fail to implement new technologies altogether.