# Maurer School of Law: Indiana University Digital Repository @ Maurer Law

Theses and Dissertations

Student Scholarship

8-2015

# Public Video Surveillance and the Separation of Powers

Lianhan Zhang Indiana University Maurer School of Law, zhanglianhan@icloud.com

Follow this and additional works at: http://www.repository.law.indiana.edu/etd Part of the <u>National Security Law Commons</u>

#### **Recommended** Citation

Zhang, Lianhan, "Public Video Surveillance and the Separation of Powers" (2015). Theses and Dissertations. Paper 26.

This Thesis is brought to you for free and open access by the Student Scholarship at Digital Repository @ Maurer Law. It has been accepted for inclusion in Theses and Dissertations by an authorized administrator of Digital Repository @ Maurer Law. For more information, please contact wattn@indiana.edu.



# PUBLIC VIDEO SURVEILLANCE AND THE SEPARATION OF POWERS

Lianhan Zhang

Submitted to the faculty of Indiana University Maurer School of Law

in partial fulfillment of the requirements

for the degree

Master of Laws – Thesis

August 2015

#### ACKNOWLEDGEMENT

The completion of this thesis could not have been possible without the support and help from so many people.

First of all, I would like to express my deepest gratitude to my advisor, Professor Ryan W. Scott for his guidance and advice. I would like to thank him for his extreme patience in the face of numerous obstacles in the process of writing and modification and for his wisdom in pushing me farther than I thought I could go.

I express my sincere appreciation to Professor Aviva A. Orenstein for always listening and giving me constant encouragement. I would also like to thank Professor Fred H. Cate and Professor Jeannine Bell for helping me with my coursework and academic research. I have learned about critical thinking on my thesis topic in their classes.

There are so many other people to thank for helping me during the last year. So many have made my stay in Bloomington a lot easier than I thought it was going to be. I am grateful to Professor Lisa Farnsworth who taught me how to think and write academically as well as how to get balance between life and study. Thanks also go to Dean Lesley Davis, Ms. Lara Gose and Ms. Allison Foust for their continuous support and help.

I would like to take this opportunity to thank my parents and my husband for their unconditional love and support, without them I would not be able to do anything.

# TABLE OF CONTENTS

INTRODUCTION	3
I. A BRIEF OVERVIEW OF PUBLIC VIDEO SURVEILLANCE AND PRIVACY	7
A. PERVASIVE VIDEO SURVEILLANCE IN THE U.S. AND ABROAD	7
The history and mechanism of the video surveillance system	
New technologies and the future of total surveillance	
The purpose of the public video surveillance and the effectiveness evaluation	
B. THREATS TO PRIVACY	
II. DEADLOCK IN RESPONDING TO VIDEO SURVEILLANCE	21
A. JUDICIAL REVIEW OF VIDEO SURVEILLANCE	
Fourth Amendment	
FOIA	25
B. SELF-RESTRAINT BY THE EXECUTIVE BRANCH	
Intra-department Guidelines	
Lack of Constraint	30
C. LEGISLATION AT THE NATIONAL, STATE, AND LOCAL LEVEL	
D. OBSTACLES TO MEANINGFUL REGULATION OF VIDEO SURVEILLANCE	
Lack of public debate	33
The interest of the industry	
Public safety perspective	
<b>III. STRENGTHS AND LIMITS OF THE JUDICIAL AND LEGISLATIVE BRANCHES</b>	
A. JUDICIAL BRANCH	
The position to set a uniform standard	
Discussion	
B. LEGISLATIVE BRANCH	
Legislation in Britain	43
Legislation in the United States	47
Discussion	
<b>IV. A COMPARATIVE PERSPECTIVE ON THE STRUCTURE OF THE EXECUTIVE BRANC</b>	H AND
REGULATIONS OF VIDEO SURVEILLANCE	56
A. ADMINISTRATIVE REGULATIONS IN DIFFERENT COUNTRIES	57
B. STRUCTURAL DIFFERENCES MATTER	59
Central control analysis (vertical factor)	60
Stakeholder analysis (horizontal factor)	
Effectiveness analysis (internal factor)	
The public attitude analysis (external factor)	
V. CONCLUSION	77
BIBLIOGRAPHY	79

# Introduction

Today, "you are being watched" is not just found in Orwell's 1984. It is a part of daily life experienced by hundreds of millions of people around the world. The most famous example is Britain. According to a commonly quoted statistic, around 2000 there were 4.2 million closed circuit television (CCTV) cameras in Britain—one for every fourteen people—and a person can be captured on over three hundred cameras each day.<sup>1</sup> Although this figure was doubted in a study in 2011, which said that the number of cameras is approximately 1.85 million and the number of times the average person is likely to be less than 70,<sup>2</sup> even those reduced figures represents a shocking level of surveillance. Despite a later start and more fragmented implementation, the United States will soon face similar challenges as video surveillance systems in the United States have grown rapidly, especially in metropolitan cities.

In Washington D.C., the seat of the nation's government and home to many critical assets, the government adopted more than 5,200 cameras in its CCTV program in 2008.<sup>3</sup> As of 2010, New York City was estimated to be continuously scanning at least 1,159 public and private cameras; "it has added 500 new cameras to subway systems in the city and has plans to add approximately 1,800 more image-capturing devices in lower and midtown Manhattan."<sup>4</sup> And the New York Police

<sup>&</sup>lt;sup>1</sup> SURVEILLANCE STUDIES NETWORK, A REPORT ON THE SURVEILLANCE SOCIETY 19 (David M. Wood ed., 2006) (U.K.), *available at* http://news.bbc.co.uk/2/shared/bsp/hi/pdfs/02\_11\_06\_surveillance.pdf.

<sup>&</sup>lt;sup>2</sup> Gerrard G, Thompson R., Two Million Cameras in the UK. CCTV IMAGE, 2011, 42(10): e2. (U.K.).

<sup>&</sup>lt;sup>3</sup> Aileen B. Xenakis , *Washington And CCTV: It's 2010, not 1984*, 42 CASE W. RES. J. INT'L L. 573, (2010), (citing Press Release, District of Columbia, Mayor Fenty Launches VIPS Program; New System Will Consolidate City's Closed-Circuit TV Monitoring (Apr. 8, 2008), http://www.dc.gov/mayor/news/release.asp?id=1273.)

<sup>&</sup>lt;sup>4</sup> Olivia J. Greer, *No Cause of Action: Video Surveillance in New York City*, 18 MICH. TELECOMM. & TECH. L. REV. 589, 595 (2012), (citing Press Release, Office of the Mayor, Mayor Bloomberg, Police Commissioner Kelly, and MTA Chairman Walder Activate Security Cameras Inside Times Square, Penn Station, and Grand Central Subway

Department (NYPD) still wants to significantly increase that amount.<sup>5</sup> In the American Civil Liberties Union's (ACLU) report on video surveillance published in February 2011, the City of Chicago was estimated to own or have an access to as many as 10,000 cameras.<sup>6</sup> In 2012, an officer in Chicago Office of Emergency Management and Communications acknowledged that the Chicago police had already got access to 20,000 video feeds from public and private sources.<sup>7</sup>

Compared with the rapid implementation of video surveillance systems in the United States, the protection of civil liberties in this field has been making little progress. In 2011, ACLU published the report calling for a moratorium on the expansion of Chicago's camera system, as well as pending a thorough and open review. This report also proposed new privacy rules for regulating all cameras. But Chicago did not adopt the ACLU's core proposals. Instead, it has installed thousands of new cameras since 2011, and plans to install more. What is worse, a new City ordinance has granted the Mayor power to purchase and install cameras without City Council approval or review. And a bill that would have required state and local government to disclose their total numbers of cameras failed.<sup>8</sup> The situation is similar in other major cities. In 2011, the New York Civil Liberties Union (NYCLU) brought an action against the U.S. Department of Homeland Security (DHS) under the federal Freedom of Information Act (FOIA), seeking documents related to a video surveillance program in lower Manhattan initiated by the NYPD. DHS was the defendant because the NYPD received grant funding from it. But the court did not

Stations as Part of NYPD's Midtown Manhattan Security Initiative (Sept. 20, 2010)).

<sup>&</sup>lt;sup>5</sup> According to the NYPD Commissioner Ray Kelly, Keith Proctor, *The Great Surveillance Boom*, FORTUNE, April 26, 2013, http://fortune.com/2013/04/26/the-great-surveillance-boom/.

<sup>&</sup>lt;sup>6</sup> Adam Schwartz, *Chicago's Video Surveillance Cameras: A Pervasive and Poorly Regulated Threat to Our Privacy*, 11 NW. J. TECH. & INTELL. PROP. 47, 48 (2013).

<sup>&</sup>lt;sup>7</sup> Hilton Collins, *Video Camera Networks Link Real-time Partners in Crime Solving*, GOVT. TECH. (Feb, 1, 2012) (citing Ruben Madrigal, OEMC Deputy Director, for the proposition: "In all, police have access to 20,000 video feeds from public and private sources."), http://www.govtech.com/public-safety/Video-Camera-Networks-Link-Real-Time-Partners-in-Crime-Solving.html.

<sup>&</sup>lt;sup>8</sup> Schwartz, *supra* note 5, at 47-48.

grant NYCLU's request, instead holding that the information about the numbers and name of assets was not subject to disclosure under FOIA exemption 7(E).<sup>9</sup>

Does it really matter that we are being watched in the public places without knowing who is behind the cameras, as long as we do not have reasonable expectation of privacy in public under the judgment of the Supreme Court?<sup>10</sup> Professor Daniel J. Solove, in his book *Nothing to Hide*, describes the Supreme Court's conception of privacy as "a form of total secrecy.<sup>11</sup> Under that secrecy paradigm, people cannot expect privacy if they expose their information in any way. But Solove contends that this interpretation does not fairly match today's social expectation of privacy in information in any way.<sup>12</sup> The Court's approach thus limits people's freedom, especially when people are engaging in political protest or dissent. "The problem with the secrecy paradigm," Solove argues, "is that we do expect some degree of privacy in public."<sup>13</sup> When people are in public, they expect that they won't be followed around or secretly recorded. Justice Alito, in his concurring opinion in *United States v. Jones*,<sup>14</sup> raised similar concerns that the use of longer term monitoring impinges on people's expectations of privacy.

Moreover, the development of new technologies would make the monitoring more systematic and more intrusive. Video surveillance is a crucial part of the government's surveillance system and is being used alongside other powerful technologies, such as biometric technologies,<sup>15</sup> telecommunications, digital computer technologies, and tagging and tracking technologies. In combination with emerging technologies, such as automatic license plate recognition (ALPR),

<sup>&</sup>lt;sup>9</sup> N.Y. Civil Liberties Union v. Dep't of Homeland Sec., 771 F. Supp. 2d 289 (S.D.N.Y. 2011)

<sup>&</sup>lt;sup>10</sup> California v. Ciraolo, 476 U.S. 207, 215 (1986).

<sup>&</sup>lt;sup>11</sup> DANIEL J. SOLOVE, NOTHING TO HIDE 100 (2011).

<sup>&</sup>lt;sup>12</sup> Jerry Kang, Information Privacy in Cyberspace Transactions, 50 STAN. L. REV. 1193, 1260 (1998).

<sup>&</sup>lt;sup>13</sup> SOLOVE, *supra* note 11, at 178.

<sup>&</sup>lt;sup>14</sup> United States v. Jones, 132 S. Ct. 945 (2012) (Alito, J., concurring).

<sup>&</sup>lt;sup>15</sup> Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 MINN. L. REV. 407, 408 (2012).

facial recognition software, and third-party databases, the video surveillance system could become extremely powerful as a highly efficient investigation tool, which could be used either for legal purposes or illegitimate ones merely based on the user's will. Keith Proctor predicts that "[t]he future of surveillance is 'video analytics,' where computers will automatically analyze camera feeds to count people, register temperature changes, and, via statistical algorithms, identify suspicious behavior."<sup>16</sup> In this way, "prediction and scoring of individuals' risk of criminal behavior" will magnify the harm to privacy.<sup>17</sup>

The pervasive and technologically sophisticated nature of modern surveillance is the outcome of bureaucracy and the desire for efficiency, speed, control and coordination. In other words, the surveillance originated from the government for the good of society. Yet its power and the possibility of abuse are worrisome. As scholars who have examined surveillance in Britain have observed, "the surveillance society" requires special vigilance from those who care about human and civil rights.<sup>18</sup>

To date, however, no branch of government has taken any meaningful action. At the national, state, and local level, governments have done little to seriously regulate surveillance. This paper aims at finding out why that is the case and explores possible ways to go in the future. Part I describes the general status of pervasive video surveillance in the United States and abroad, as well as the threats it poses to the privacy. Part II focuses on the deadlock responding to regulation

<sup>&</sup>lt;sup>16</sup> Proctor, *supra* note 5.

<sup>&</sup>lt;sup>17</sup> Kevin Miller, *Total Surveillance, Big Data, and Predictive Crime Technology: Privacy's Perfect Storm*, 19 J. TECH. L. & POL'Y 105, 106 (2014).

<sup>&</sup>lt;sup>18</sup> First, large-scale technological infrastructures are peculiarly prone to large-scale problems. Second, it is equally important to remember the point about the corruptions and skewed visions of power. Third, all true surveillance systems are meant to discriminate between one group and another, and it is difficult for the problem to be brought into open when high-technology is involved. Fourth, the surveillance might undermine the social relationship which depends on trust. Finally, the surveillance distracts people from alternatives and from larger and more urgent questions. It is still a question whether this is really the best way of pursuing these goals. SURVEILLANCE STUDIES NETWORK, *supra* note 1, at 2-4.

of video surveillance, including responses of three branches of government in the United States and among the public. Part III analyzes the factors lying in the three branches that would impede taking actions, compares the practice in the United States with experience in other countries, and tries to find a weakest point to break the deadlock. In Part IV, this paper concludes that public participation is the key to breaking through the deadlock in light of the democratic political structure in the United States. Part V is the conclusion.

# I. A Brief Overview of Public Video Surveillance and Privacy

# A. Pervasive Video Surveillance in the U.S. and Abroad

## The history and mechanism of the video surveillance system

Public video surveillance using CCTV has a history of more than 50 years. In September 1968, Olean, New York became the first city in the United States to install video cameras along its main business street to fight crime.<sup>19</sup> Contrary to its reputation, Britain is not the first country to adopt CCTV in public places. It started its first permanent and systematic use of public CCTV in 1975, when London Transport introduced CCTV into the Subway system. Before that, CCTV was mainly deployed in the private sector businesses such as retail stores and supermarkets.<sup>20</sup> During the 1980s, video surveillance began to diffuse, specifically focusing on crime prevention in public areas. In the 1990s, digitalization and the introduction of video analytics transferred CCTV from

<sup>&</sup>lt;sup>19</sup> Robb, Gary C., *Police Use of CCTV Surveillance: Constitutional Implications and Proposed Regulations*, U. MICH. J. L. REFORM, 572, (1979).

<sup>&</sup>lt;sup>20</sup> McCahill M, Norris C. CCTV in Britain. Center for Criminology and Criminal Justice-University of Hull, 2002: 1-70, 8. (U.K.).

sole video transmission (and data recording) to distributed camera systems that are capable of performing low-level analysis in real time. Now, video surveillance has gone to the "second generation surveillance," which shows "the change from a dumb camera that needs a human eye to evaluate its images to a computer–linked camera system that evaluates its own video images.<sup>21</sup>

The explosive growth of CCTV implementation globally has been possible because of dropping camera prices and increasing network connectivity. Although it is difficult to judge the exact number of surveillance cameras in each country due to lack of any register of publicly owned cameras and issues of private ownership,<sup>22</sup> there is clear evidence of massive deployments taking place in North America, China, and Europe.<sup>23</sup>

Over this long period, the content of the concept "video surveillance" has kept evolving with the development of technology, as well as the promise and expectations of video surveillance. As Professor Bernhard Rinner explains:

The main objective in the early days was simply to extend the visual sensing capabilities of the observer to the site of interest, while recent surveillance systems are expected to perform complex analysis tasks with the goal to understand what is going on in the monitored area.<sup>24</sup>

Today, most public CCTV video surveillance systems are cameras utilizing digital video recorders (DVRs) transmitting signals to a centralized setting, actively and remotely monitored by security personnel in a control room, or passively taped for future viewing if needed. This is different from the earliest systems involved constant monitoring because there was no way to record and store information.

<sup>&</sup>lt;sup>21</sup> Surette R., The thinking eye: *Pros and cons of second generation CCTV surveillance systems*. 28(1), POLICING: INT'L J. POLICE STRATEGIES & MGMT., 152 (2005)

<sup>&</sup>lt;sup>22</sup> Kroener I., "Caught on Camera": The media representation of video surveillance in relation to the 2005 London Underground bombings. 11(1/2) SURVEILLANCE & SOC'Y, 121 (2013). (U.K.).

<sup>&</sup>lt;sup>23</sup> Porikli F, Brémond F, Dockstader S L, et al. *Video surveillance: past, present, and now the future*. 30(3) IEEE SIGNAL PROCESSING MAGAZINE, 190, 190 (2013).

<sup>&</sup>lt;sup>24</sup> *Id*.at 191.

Over the last few decades, CCTV technologies have evolved into a combination of sophisticated video equipment technologies and software technologies. Regarding the equipment, innovations including "night vision cameras, computer assisted operations, and motion detectors that allow an operator to instruct a system to go on 'red alert' when anything moves in view of the cameras" have considerably enhanced surveillance systems.<sup>25</sup> There have been technologies to protect camera lenses such as bulletproof casing and automated self defense mechanisms. Furthermore, picture clarity has improved (many cameras are able to read a cigarette package label at a hundred meters), while digital compact disk quality and the capabilities like zooming in, panning, and tilting have helped make the system more powerful. At the same time, cameras have also been becoming smaller and cheaper.<sup>26</sup>

Software technologies also play a crucial role in what is called "automated video surveillance."<sup>27</sup> As early as the 1960s, there have been patents in the United States describing a television system for detection of differences,<sup>28</sup> and a television surveillance system that outputs an alarm by using the differences between the sample data and data average.<sup>29</sup> However, even today, the promise of video content analysis with computers has not been fulfilled. The content of video surveillance still depends on manual analysis. Thus, a tension appears between an enormous and ever-increasing store of data—far more than any human can ever view or analyze—with the limited number of human operators and the lack of constant attention.<sup>30</sup> One solution being explored is crowd sourcing for content analysis.<sup>31</sup> Others include advanced analytics and

<sup>&</sup>lt;sup>25</sup> Nieto M, Johnston-Dodds K, Simmons C W., PUBLIC AND PRIVATE APPLICATIONS OF VIDEO SURVEILLANCE AND BIOMETRIC TECHNOLOGIES 3-4 (California State Library, California Research Bureau) (2002).

<sup>&</sup>lt;sup>26</sup> *Id*, at 4.

<sup>&</sup>lt;sup>27</sup> Porikli, *supra* note 23, at 191.

<sup>&</sup>lt;sup>28</sup> U.S. Patent 3114797, 1963.

<sup>&</sup>lt;sup>29</sup> U.S. Patent 3590151, 1966.

<sup>&</sup>lt;sup>30</sup> Porikli, *supra* note 23, at 192.

<sup>&</sup>lt;sup>31</sup> Crowd sourcing refers to the use of the footage by placing it on social media, resulting in a groundbreaking

processing in which algorithms help to distill the data into useful intelligence.<sup>32</sup>

#### New technologies and the future of total surveillance

Contrary to the argument that video cameras are "no different from a pair of eyes,"<sup>33</sup> the true power of video surveillance lies in the fact that the system can transcend the ordinary power of human observation with the ability to zoom in, track, record and analyze. Cameras are connected together and people's acts everywhere can be recorded into an integrated system. In this system, the most powerful tool for law enforcement is known as facial recognition technology, which automatically matches the faces of surveilled individuals to known target faces in a comparison database, and provides an alert when a target hit appears. With this technology, the operator can identify a person of interest in a crowd within a few seconds, and acquire all acts that person has done recently to draw a whole map of his or her public activities. Public use of face recognition systems was first launched in the London borough of Newham in 1998. In the United States, the failure of traditional security measures to prevent the 9/11 terrorist attacks has spurred the adoption of facial recognition systems in airports and other public places.<sup>34</sup>

Although NYPD guidelines indicate that the police will refrain from using facial recognition technology, they do not guarantee this technology will not be used forever. Patent activity alone demonstrates that the technology has come of age. Between 1970 and 1995, the U.S. Patent Office granted fewer than 10 patents involving facial recognition. Between 2001 and 2011, the number leapt to 633. These patents are increasingly focused on, and applicable to, law enforcement and

collaboration between the police and the public.

<sup>&</sup>lt;sup>32</sup> Porikli, *supra* note 23, at 192.

<sup>&</sup>lt;sup>33</sup> Siegel L, Perry R A, Gram M H, *Who's Watching? Video Camera Surveillance in New York City and the Need for Public Oversight*. A Special Report by the New York Civil Liberties Union, (2006),

http://www.nyclu.org/pdfs/surveillance\_cams\_report\_121306.pdf.

<sup>&</sup>lt;sup>34</sup> Surette, *supra* note 21.

national security.<sup>35</sup> At the same time, despite some doubts about its accuracy rates in some circumstances,<sup>36</sup> facial recognition has been discussed heatedly in the technologies field.<sup>37</sup> There is considerable research underway aimed at overcoming the shortcomings.<sup>38</sup> And facial recognition is also the first step in one of the most active topics in computer science: human motion analysis, which concerns mainly detection, tracking and recognition of human behavior.<sup>39</sup>

Video cameras are considered the prototypical method of surveillance, but there are also a variety of other emerging technologies that, when combined, could create an inescapable net of total surveillance. Such technologies include automated license plate recognition (ALPR) systems and biometric technologies. ALPR systems can scan and track the movements of vehicles. According to one survey with responses from over 70 agencies in 2012, 85% of responding police departments had implemented or expected to implement ALPR within the next five years.<sup>40</sup> Biometric-based identity management systems are considered to augment or supersede existing identity verification tools. A biometric database, for instance, could potentially require the collection of the digital photos, fingerprints, iris scans, and/or DNA of all citizens and noncitizens.41

When location and biometric data is unified in centralized repositories along with other data

Best-Rowden L, Han H, Otto C, et al. Unconstrained face recognition: Identifying a person of interest from a media collection, Information Forensics and Security, IEEE Transactions on, 2014, 9(12): 2144-2157.(U.K.).

<sup>&</sup>lt;sup>35</sup> Laura K. Donohue, Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age, 97 Minn. L. Rev. 407, 410 (2012).

<sup>&</sup>lt;sup>36</sup> Klontz J C, Jain A K, A case study on unconstrained facial recognition using the boston marathon bombings suspects, 13 Michigan State University Technical Report MSUCSE, 4 (2013).

<sup>&</sup>lt;sup>37</sup> Generally see, Wechsler, Harry, et al., eds. Face recognition: From theory to applications, 163 SPRINGER SCIENCE & BUSINESS MEDIA, (2012).

<sup>&</sup>lt;sup>38</sup> eg. Pagano C, Granger E, Sabourin R, et al. Adaptive ensembles for face recognition in changing video surveillance environments, 286 INFORMATION SCIENCES, 75 (2014);

<sup>&</sup>lt;sup>39</sup> Bhaltilak K V, Kaur H, Khosla C., Human Motion Analysis with the Help of Video Surveillance: A Review, 4(9) INT'L J. COMPUTER SCI. ENGINEERING TECH (IJCSET), 245 (2014).

<sup>&</sup>lt;sup>40</sup> Police Executive Research Forum, How Are Innovations in Technology Transforming Policing?, PERF Critical Issues in Policing Series report (2012), available at http://policeforum.org/library/critical-issues-inpolicingseries/Technology\_web2.pdf. <sup>41</sup> Margaret Hu, *Biometric Id Cybersurveillance*, 88 IND. L.J. 1475, 1477 (2013).

collected by the government and private entities, ranging from mobile camera phones used by the public and hand-held cameras used by police patrols on city streets to conventional telecommunication data, it creates large data sets from which meaningful information could be distilled. "Big data analysis" uses computation to examine large data sets for correlations, to turn a morass of data into useful information. The future of total surveillance is predictive systems built on big data, which can identify patterns by correlations from the past events or individual behaviors or generalized high crime areas, with the goal of complete pre-crime prediction. In the book and film *Minority Report*, which no discussion of the predictive systems could bypass, a dystopia might become the reality where the police feel comfortable in arresting people for what they are foreseen to do.<sup>42</sup> The only difference is the prediction in *Minority Report* relies on clairvoyants, while the prediction in the future real world might be computers with surveillance feeders. <sup>43</sup>

#### The purpose of the public video surveillance and the effectiveness evaluation

Despite those risks, in the worldwide context, the public video surveillance systems are very popular and have received widespread support from politicians, policy-makers and citizens. Surveillance is advertised as a way to combat terrorism, to deter and detect crime, to prevent disorder and antisocial behavior, and more generally to make people feel safer. Public video surveillance is said to be a cost-effective investigational tool, which can help speed up investigations and encourage offenders to plead guilty. The police can use it to identify offenders, witnesses, to prove or disprove alibis and versions of events, or to provide evidence for trials. Moreover, cameras in public places could also be used as an administrative and social-management tool for deploying officers more effectively, to monitor incidents and suspicious

<sup>&</sup>lt;sup>42</sup> Spielberg, Steven, and Philip K. Dick. *Minority Report*. California: Dreamworks, 2002.

<sup>&</sup>lt;sup>43</sup> Miller, *supra* note 17, at 113.

behavior, to allow early interventions to reduce the severity of incidents, and to provide guidance for officers on the scene. In addition, prominent cameras in highly visible locations are presumed to have a deterrent effect on potential offenders.<sup>44</sup>

One remarkable example is the use of the video surveillance following the Boston Marathon bombing event on April 15, 2013. "The massive number of cell phones and closed circuit cameras on the street provide an incredible wealth of video and photo."<sup>45</sup> It was only 88 hours before the suspects were positively identified.<sup>46</sup>

Although combatting crime and terrorism are the most important goals of surveillance systems, many people take the impacts of public video surveillance for granted. In fact, evidence on the effectiveness of the public video surveillance is still inconclusive and fairly contradictory. A systematic review that summarized 46 relevant studies from both the USA and Britain on the effectiveness of CCTV in crime reduction in 2002, according to strict methodological criteria, concluded that CCTV reduces crime only to a small degree; that it is most effective in reducing vehicle crime in car parks or parking lots; and that it has little or no effect on crime in public transport and city center settings.<sup>47</sup> These conclusions are consistent with earlier research, which argued that anti-crime policy aiming at serious crimes such as terrorism had become, in practice, more often applied to less serious behavior and antisocial activities (like littering, public urinating, traffic control, drunkenness, parking violations, and public smoking).<sup>48</sup> Meanwhile, other research indicates that, instead of deterring or preventing crime, surveillance merely displaces crime in

<sup>&</sup>lt;sup>44</sup> LEVESLEY T, MARTIN A, BRITAIN G. POLICE ATTITUDES TO AND USE OF CCTV, (Home Office, 2005). (U.K.). <sup>45</sup> M. Stroud. *In Boston bombing, flood of digital evidence is a blessing and a curse*. THE VERGE, April 16, 2013, http://www.theverge.com/2013/4/16/4230820/in-boston-bombing-flood-of-digital-evidence-is-a-blessing-and-acurse.

<sup>&</sup>lt;sup>46</sup> Klontz, *supra* note 36, at 4.

<sup>&</sup>lt;sup>47</sup> WELSH B C, FARRINGTON D P, CRIME PREVENTION EFFECTS OF CLOSED CIRCUIT TELEVISION: A SYSTEMATIC REVIEW, Home Office, 2002 (U.K.).

<sup>&</sup>lt;sup>48</sup> Campbell, D. and Ross, L., *The Connecticut crackdown on speeding*, 3 LAW & SOC'Y REV., 33 (1968).

various forms.49

Because Britain is at the forefront of using cameras to monitor public space, most of understanding on the effects of cameras is based on Britain's experience and research. Perhaps surprisingly, CCTV in Britain was introduced and largely implemented before 1994, prior to any systematic evaluation of its effectiveness in reducing crimes.<sup>50</sup> Since then, there have been positive findings as well as negative findings. A study in 1999 found a reduction of 25% crime rates sustained a period over two years.<sup>51</sup> That was undoubtedly a successful example, but a rare one. According to an analysis by Dr. Michael McCahill and Professor Clive Norris, no other studies had shown the same consistent and positive results. Instead, some studies had found CCTV has no overall impact, and that both functional and geographical displacements existed.<sup>52</sup>

Although even fewer studies in the United States have examined the effectiveness of public video surveillance, existing research shows a consensus that the implementation of public video surveillance might have impact on the crime rates, but a number of involving factors are complicated and intertwined, such as the type of crime in question, the location of the cameras, the concentration of cameras, monitoring practices, and the study design.

For example, a study in 2009 shows the effects of public surveillance cameras in Philadelphia. Despite variation across individual camera sites, serious crime decreased by about 5% in the post-intervention period, and disorder crimes decreased by 16%. When serious and disorder crime were analyzed together, the camera implementation was associated with a 13% decline in the post-intervention period.<sup>53</sup> Another empirical study in Schenectady, examining an area of 10 square

<sup>&</sup>lt;sup>49</sup> Clarke, M., Blind eye on the street?, POLICE REV., August, 29 (1994).

<sup>&</sup>lt;sup>50</sup> McCahill, *supra* note 20.

<sup>&</sup>lt;sup>51</sup> Armitage R, Smyth G, Pease K, *Burnley CCTV evaluation*, Surveillance of public space: CCTV, street lighting and crime prevention, 1999, 10: 225-50. (U.K.).

<sup>&</sup>lt;sup>52</sup> McCahill, *supra* note 20, at 8.

<sup>&</sup>lt;sup>53</sup> Ratcliffe, J., Taniguchi, T., & Taylor, R. B, The crime reduction effects of public CCTV cameras:

miles with a population of more than 60,000, revealed that "the surveillance cameras have had effects on overall crime levels. But these effects have not been achieved consistently."<sup>54</sup> Cameras are more often associated with declines in personal crime, rather than property crime.<sup>55</sup> And the findings may reflect that there is an interactive relationship between camera surveillance and the nature of the location as well as the nature of offenses in those locations. But cameras appear to be successful at reducing disorder, which is similar to the effectiveness of cameras elsewhere in the United States.<sup>56</sup>

After the 9/11 attacks, actual or potential terrorist incidences justified calls for increased using of public video surveillance. Yet one study has concluded that the installation of cameras has a relatively smaller deterrent effect on terrorism than on other forms of crime."<sup>57</sup> In fact, as one summary of the existing research notes, CCTV is not chosen as a counter-terrorism tool because it is effective. "Indeed, we do not know whether they are (effective)."<sup>58</sup> In this article, the authors also indicate that U.S. police agencies do not regularly employ surveillance interventions for the specific purpose of countering terrorism. They view Department of Homeland Security grants as

A multi-method spatial approach. 26 JUSTICE QUARTERLY, 746 (2009).

<sup>&</sup>lt;sup>54</sup> McLean S J, Worden R E, Kim M S., *Here's Looking at You An Evaluation of Public CCTV Cameras and Their Effects on Crime and Disorder*, 38(3) CRIM. JUSTICE REV., 303, (2013).

<sup>&</sup>lt;sup>55</sup>Numerous previous studies by independent scholars have concluded that video surveillance cameras in fact do not reduce violent crime, and only in certain circumstances reduce property crime. A 2008 study of Los Angeles' cameras, by the University of Southern California ("USC"), found no statistically significant impact on violent crime, property crime, or quality of life crime (such as prostitution or public drunkenness). A 2009 study of San Francisco's cameras, by the University of California at Berkeley, found no statistically significant impact on violent crime, drug crime, or quality of life crime, and some impact on property crime. A 2005 review of 13 studies in England found no statistically significant impact on violent crime, and a statistically significant reduction in property crime in only two of the thirteen locations studied, one of which was a parking lot. A 2008 review by USC of 44 studies in the United States and abroad concluded that none of the domestic studies found a statistically significant impact on crime, and that any impact found in foreign studies was limited to property crime. See, ACLU of Illinois, *Chicago's Video Surveillance Cameras: A Pervasive and Unregulated Threat to Our Privacy*, Feb. 2011, http://il.aclu.org/site/DocServer/Surveillance\_Camera\_Report1.pdf?docID=3261.

<sup>&</sup>lt;sup>56</sup> McLean, *supra* note 54, at 303.

<sup>&</sup>lt;sup>57</sup> Stutzer A, Zehnder M. *Is camera surveillance an effective measure of counterterrorism?* 24(1) DEF. & PEACE ECON., (2013).

<sup>&</sup>lt;sup>58</sup> Lum C, Haberfeld M M, Fachner G, et al. *Police activities to counter terrorism: What we know and what we need to know*, in TO PROTECT AND TO SERVE, 101, 111 (David Weisburd et al. ed., 2011).

recent efforts to increase the use of technologies by police agencies for counterterrorism purposes. Thus they suggest that "if governments wish to increase the use of technologies in law enforcement efforts against terrorism, not only must they be willing to fund such efforts, but technologies must also be shown, through evaluation, to be effective, cost effective, and easy to use and operate."<sup>59</sup>

Although most research focuses on crime rates, there are also studies emphasizing the sociological processes of video surveillance as a policy tool increasingly deployed in the security field. Professor Clive Norris in his study illustrated that the symbolic value of CCTV was most important because its visibility could send a message to the public that the government was doing something about the crime problem.<sup>60</sup>

## **B.** Threats to Privacy

Public video surveillance has more than one facet that may invade people's rights protected by the Constitution. One main facet is the information privacy, which is frequently discussed in the video surveillance field. However, pervasive public video surveillance involves a variety of human behaviors, the body, use of space and other facts of privacy. The values relevant to those behaviors transcend the mere value of protecting the personal information.

Consider the following examples of threats people may face without adequate oversight of public video surveillance:

1. Recorded surveillance footage may be private or embarrassing, even if it records public movements and activities (e.g. medical appointments, romantic liaisons, social activities). The

<sup>&</sup>lt;sup>59</sup> Id. at 120.

<sup>&</sup>lt;sup>60</sup> Norris, McCahill and Wood, *The Growth of CCTV: a global perspective on the international diffusion of video surveillance in publicly accessible space*, SURVEILLANCE & SOC'Y, 125 (2004), http://www.surveillance-and-society.org/cctv.htm

Supreme Court has long held that it is unconstitutional for the government to require that individuals identify themselves while speaking in public or to require the disclosure of membership lists.<sup>61</sup> But a video camera deployed on the entrance of a building could easily reveal the members of the organization as clear as a membership list.<sup>62</sup> Furthermore, cameras have the ability to cross the line between the public and the private. Here is how Sarah Duguid, a *Financial Times* reporter, described her experience with a London police camera operator: "He zooms in on three young men wearing baseball caps. He gets so close to them that I can read the brand of their mobile phone. 'Theoretically,' explained the operator, 'I could read a text message from here.'"<sup>63</sup> The same thing occurs in the United States. Most Chicago surveillance cameras can be used to zoom in to see small objects at great distances, thus they can also be used to aim at particular members of the public.<sup>64</sup>

2. Cameras may be misused or recordings leaked by officers. As another journalist explained in 2001 after observing a camera control room in Great Britain: "When you put a group of bored, unsupervised men in front of live video screens and allow them to zoom in on whatever happens to catch their eyes, they tend to spend a fair amount of time leering at women."<sup>65</sup> Both in Britain and the United States, there were reports of officers improperly manipulating surveillance cameras to focus in on women's breasts and buttocks.<sup>66</sup> There have also been high-

<sup>&</sup>lt;sup>61</sup> See Buckley v. Am. Constitutional Law Found, 525 U,S, 182 (1992); NAACP v. Alabama ex rel. Patterson, 357 U.S. 449 (1958).

<sup>&</sup>lt;sup>62</sup> Olivia J. Greer, *No Cause of Action: Video Surveillance in New York City*, 18 MICH. TELECOMM. & TECH. L. REV. 589, 610-11 (2012).

<sup>&</sup>lt;sup>63</sup> Siegel, *supra* note 33.

<sup>&</sup>lt;sup>64</sup> Schwartz, supra note 6, at 57.

<sup>&</sup>lt;sup>65</sup> ACLU of Illinois, *Chicago's Video Surveillance Cameras: A Pervasive and Unregulated Threat to Our Privacy*, Feb. 2011, http://il.aclu.org/site/DocServer/Surveillance\_Camera\_Report1.pdf?docID=3261.

<sup>&</sup>lt;sup>66</sup> See, Jeffrey Rosen, *A Watchful State*, N.Y. TIMES, Oct. 7, 2001; Andrew Parker, *Perveillance of CCTV Operator*, THE SUN, Feb. 14, 2007; *Spy cameras fail to focus on street crime*, THE WASH. TIMES, Aug. 13, 2006; Jaxon Van Derbeken, *9-month Suspension for Police Officer*, S.F. CHRON., Apr. 22, 2005. 33; Jon Gargis, *Strip Traffic Camera Follows Pedestrians Home*, THE CRIMSON WHITE, Sept. 15, 2003; Sarah Wallace, *NYPD Housing Surveillance Staffed by Cops Under Investigation*, ABC NEWS, Apr. 23, 2004.

profile examples of recordings and other information being leaked. In one notorious case, the State of Florida had been selling photographic images and other personal information stored on driver's license to commercial marketers. <sup>67</sup> In the Bronx, a young man's suicide in the elevator was caught on one of the 200 closed-circuit cameras set up in city housing projects as part of the NYPD's Video Interactive Patrol Enhances Response program. A police officer emailed this recording to his friend, and the recording was later posted on a porn website.<sup>68</sup> In Indiana, a school technician was arrested after he forwarded to his home computer images of students taken by a school video surveillance camera.<sup>69</sup> In Washington, a video surveillance camera in a high school captured two girls kissing and holding hands, and the dean of students shared video of the incident with one of the girl's parents.<sup>70</sup> Some breaches can and do occur even with clear rules and procedures in place.<sup>71</sup> In addition, improper access poses serious risks. In practice, people not properly authorized to view or work with data about individuals could be involved rather than only trained security personnel who are supposed to exclusively do the monitoring job.<sup>72</sup> The potential for misuse of information could increase if data is available to people lack of privacy protection awareness. And those people are hardly held accountable if they are unidentified.

3. Cameras installed for security purposes might also be used for other purposes, even illegal ones.

http://nypost.com/2004/06/22/bx-cop-caught-in-net-suicide-video-scandal/.

John Files, V.A. Laptop Is Recovered, Its Data Intact, N.Y. TIMES, June 30, 2006.

<sup>&</sup>lt;sup>67</sup> Jonathan Mandell, *Proof of Your Existence, Complete with Bad Photo*, N.Y. TIMES, October 20, 1999.

<sup>&</sup>lt;sup>68</sup> Murray Weiss, Bronx Cop Caught in 'Net – Suicide-Video Scandal, N.Y. POST, June 22, 2004,

<sup>&</sup>lt;sup>69</sup> Vids of Students on Arrested Tech's Computer, 6 NEWS: THE INDY CHANNEL, Feb. 15, 2008,

http://www.theindychannel.com/news/education/school-vids-of-students-on-arrested-tech-s-computer

<sup>&</sup>lt;sup>70</sup> Brent Champaco, *Cameras Catch Kiss, Raising Questions*, THE NEWS TRIBUNE, Apr. 26, 2007.

<sup>&</sup>lt;sup>71</sup> The theft of a laptop computer from the home of a Veterans Administration analyst leaded to a personal information breach, including 17.5 million veterans and soldiers on active duty.

The same thing could happen where anyone who has access to electronic video archives can download images (with or without authorization) to a laptop and walk out the door.

<sup>&</sup>lt;sup>72</sup> Heenan Blaikie LLP, *Video surveillance - breach of privacy*, LEXOLOGY, December 7 2010,

http://www.lexology.com/library/detail.aspx?g=b0c1da70-e8be-4c4e-9469-780a5ca14b5e

Some may be used to sanction non-criminal behavior such as dress code infractions, smoking or drinking in prohibited areas, and dogs walking in the building.<sup>73</sup> According to NYCLU's report, the expansion beyond a project's original goals could be worse. The database could be used for illegitimate purposes, such as discrimination and bias.

In the absence of legal constraints, the illicit purposes for which video images may be used are limited only by the imagination. Police officials could create a video archive of anti-war protestors. An NYPD video unit might target black or Latino youth who enter a majority-white neighborhood. A security professional could use video records to stalk someone.<sup>74</sup>

It is shocking that only racial minorities are presented as the targets of surveillance in Chicago's training DVD for officers using the surveillance cameras.<sup>75</sup> And in a study of 592 hours of camera monitoring in England, the finding reveals black people were between 1.5 and 2.5 times more likely to be watched than one would expect from their presence in the population being monitored. Furthermore, 68% of all surveillance for "no obvious reason" is of blacks, compared to 35% of whites.<sup>76</sup>

4. Recordings could be used by the police to harass or threaten politicians or critics. After the 9/11 attacks, the police have found it easier to engage in investigating the political activities since regulations on them are loosened in the name of counter-terrorism. For instance, the Handshu Agreement, which regulates police behavior in New York City regarding political activity, was modified in 2003 in light of the heightened threat of terrorism. The standard of commencing an investigation was changed from "specific information"<sup>77</sup> indicating the crime,

<sup>&</sup>lt;sup>73</sup> Id.

<sup>&</sup>lt;sup>74</sup> Siegel, *supra* note 33.

<sup>&</sup>lt;sup>75</sup> ACLU of Illinois, *supra* note 65.

<sup>&</sup>lt;sup>76</sup> Clive Norris & Gary Armstrong, *CCTV and the Social Structuring of Surveillance*, 10 CRIME PREVENTION STUDIES, 162 (1999), http:// www.popcenter.org/library/CrimePrevention/Volume\_10/06-NorrisArmstrong.pdf.

<sup>&</sup>lt;sup>77</sup> Handschu v. Special Services Div., 605 F. Supp. 1384, 1421 (S.D.N.Y. 1985), aff 'd, 787 F.2d 828 (2d Cir. 1986).

to "information indicating the possibility of the crime."<sup>78</sup> In 2004, the Republican National Convention in New York was blanket videotaped by the NYPD,<sup>79</sup> and if the police departments retain these digital images, there is a risk that "they will serve as a permanent, 'searchable' archive—in essence, visual dossiers on dissenters."<sup>80</sup> Another example is the risk that Chicago civilians engaged in activities protected by the First Amendment could be aimed and zoomed at by the surveillance operators under Chicago police policy, based on a mere "proper law enforcement purpose." Scholars argue that this standard is too nebulous to guide officers' discretion, or to provide a meaningful framework for later review.<sup>81</sup>

- 5. Chilling effect: the very existence of surveillance might discourage lawful public activities by undermining personal autonomy. If people will be forced to constantly ask themselves when even the smallest action is taken, "Will this act look suspicious? Will my normal behavior now collected by the government and come back to haunt me someday if I become a target?" they will feel unfree and insecure. When people realize every event or statement that he might regret is recorded by the ongoing surveillance and might be viewed by others one day, their behavior will definitely be less spontaneous. In other words, someone being closely and steadily watched is very likely to feel loss of freedom and gross discomfort due to being under a magnifying glass of the government.
- 6. Facial recognition could be combined with other data sources to create a comprehensive log of a person's life, routines, habits and travels. When viewed in the aggregate, people's private thoughts or goals could be revealed by the public authorities by collecting pieces of person's

<sup>&</sup>lt;sup>78</sup> Handschu v. Special Services Div, 288 F. Supp. 2d 411, 422 (S.D.N.Y. 2003) (emphasis added) ("Second Revised Order and Judgment"). For a history of this case prior to entry of the modified consent decree, see Handschu v. Special Services Div., 273 F. Supp. 2d 327 (S.D.N.Y. 2003).

<sup>&</sup>lt;sup>79</sup> Jim Dwyer, New York Police Covertly Join In at Protest Rallies, N.Y. TIMES, Dec. 22, 2005.

<sup>&</sup>lt;sup>80</sup> Siegel, *supra* note 33.

<sup>&</sup>lt;sup>81</sup> Schwartz, *supra* note 6, at 57.

life and put them together to get a comprehensive picture of his interests. And because facial recognition or other databases could link those observations to an identity, people lose not only their privacy, but also their anonymity. The new technologies raise serious concerns because there is a qualitative difference between visual confirmation of a person's location (a naked eye theory<sup>82</sup>) and the vast history of data stored by or accessible to the government (a mosaic theory<sup>83</sup>).

# **II** . Deadlock in Responding to Video Surveillance

The threats to privacy discussed in the prior part have had some impact on the U.S. government. Until the late 1960s, local law-enforcement agencies in the U.S. had not adopted surveillance cameras because of concerns about "underdeveloped technology, excessive cost and unfavorable public opinion."<sup>84</sup> But nowadays, two of these concerns have clearly diminished, although public opinion remains mixed. Since multiple factors have spurred the vast implementation of public surveillance, most of research in this area argues for regulations rather than suggesting that video surveillance be abandoned, which is impossible. The balance is important: "for CCTV technology to be used most effectively, it must be used efficiently while

<sup>&</sup>lt;sup>82</sup> "Industry representatives and government officials who support increased video surveillance argue that video cameras are no different from a pair of eyes." Siegel, *supra* note 33.

<sup>&</sup>lt;sup>83</sup> Judge Ginsburg of the D.C. Circuit espoused the so called "mosaic theory" – the idea the certain government investigation tactics, such as tracking suspects via GPS devices or geolocation data provided by cellular phone service providers (or, presumably, other forms of data mining a wide variety of electronic records and online information), empowered the government to accumulate such a detailed digital picture of a person's life, routines, habits, and travels that the information gathering itself triggered Fourth Amendment protection, despite the fact that a search for any individual piece of the same data might not have done so because the information was in some sense publicly available. Newell, Bryce Clayton, *Local Law Enforcement Jumps on the Big Data Bandwagon: Automated License Plate Recognition Systems, Information Privacy, and Access to Government Information* (October 16, 2013). 66 ME, L. REV., 398 (2014).

<sup>&</sup>lt;sup>84</sup> Robert R. Belair & Charles D. Bock, *Police Use of Remote Camera Systems for Surveillance of Public Streets*, 4 COLUM. HUM. RTS. L. REV. 143, 147 (1972).

maintaining people's faith in government—faith that they are safe, that their taxes are being spent on programs that enhance public safety, and that their civil liberties are not being compromised in the process."<sup>85</sup>

Despite those wishes for balance, in fact, public video surveillance has not yet been under adequate regulations. Facing this new technology being implemented on a vast scale, all three branches of the U.S. government—the judicial, the executive, and the legislative—have responded poorly. None of them has taken meaningful actions to seriously regulate surveillance systems or to address the privacy issues raised by them.

# A. Judicial Review of Video Surveillance

Regarding privacy, a number of actions in the U.S. courts may place limits on excessive surveillance. Apart from describing the fact that the emerging video surveillance technologies fall outside the definition of the search under the Fourth Amendment, this part will explore actions taken under the Freedom of Information Act (FOIA) and explain why they are always struck down by the court.

#### **Fourth Amendment**

It is often argued that pervasive public video surveillance might violate the Fourth Amendment's prohibition against "unreasonable searches and seizures." As one Fourth Amendment scholar has pointed out:

[A] detective or spy wishing to build a dossier on an individual's life and personality would probably learn more from examining a searchable database of such images than he would by rummaging through a purse, wallet, or suitcase, especially if he could link from

<sup>&</sup>lt;sup>85</sup> Aileen, *supra* note 3, at 592.

the images to other information about the individual's identity and background.<sup>86</sup>

This concern, however, has not received a clear answer from the Supreme Court. The concurring opinion in the latest case *United States v. Jones*<sup>87</sup> indicates a direction where Fourth Amendment protections might go, which is to draw a constitutional distinction between short-term surveillance and prolonged, pervasive monitoring. But the current dominant precedents rule that public video surveillance does not trigger the Fourth Amendment issue.

In the landmark case *Katz v. United States*,<sup>88</sup> the Court established a two-pronged test for determining whether government's investigative activity rises to the level of a search. First, the government's conduct must offend the citizen's subjective manifestation of a privacy interest. Second, that the expectation should be one that society is prepared to recognize as "reasonable".<sup>89</sup>

Under *Katz*, people do not have reasonable expectation in public places. In *United States v. Knotts*,<sup>90</sup> the Court upheld the warrantless use of a beeper used by law enforcement to track movements of a criminal suspect. In reaching its conclusion, the Court stressed the suspect's diminished expectation to privacy in an automobile on a public thoroughfare.

When [the defendant] traveled over the public streets he voluntarily conveyed to anyone who wanted to look the fact that he was traveling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property.<sup>91</sup>

In addition, under Katz, visual inspection is not always a "search." In California v. Ciraolo,<sup>92</sup>

<sup>&</sup>lt;sup>86</sup> Marc Jonathan Blitz, *Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Tracks Image and Identity*, 82 TEX. L. REV. 1349, 1359 (2004),

http://works.bepress.com/marc\_jonathan\_blitz/15. <sup>87</sup> United States v. Jones, 132 S. Ct. 945 (2012).

<sup>&</sup>lt;sup>88</sup> Katz v. United States, 389 U.S. 347 (1967).

<sup>&</sup>lt;sup>89</sup> *Id*, Justice Harlan concurring opinion.

<sup>&</sup>lt;sup>90</sup> United States v. Knotts, 460 U.S. 276, 282 (1983).

<sup>&</sup>lt;sup>91</sup> *Id.* at 281-82.

<sup>92</sup> California v. Ciraolo, 476 U.S. 207, 207, 106 S. Ct. 1809, 1810, 90 L. Ed. 2d 210 (1986).

the Court held that the Fourth Amendment was not violated by the naked-eye aerial observation of respondent's backyard. But if the surveillance engages in more than naked-eye observation, the outcome under the Fourth Amendment may be different. In *Kyllo v. United States*<sup>93</sup> the Court held that:

[O]btaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical "intrusion into a constitutional protected area," constitutes a search—at least where the technology in question is not in general public use.

The *Katz* test has been criticized as an outmoded method in the technologically advanced society, where very little information can be kept private. Professor Stephen E. Henderson argues that the reasonable expectation of privacy test should be dropped, because "technology will lead to no privacy, and police practice will incorporate that technology to create a reality of no privacy."<sup>94</sup>

The Supreme Court, perhaps realizing the limits of the *Katz* test, returned to a kind of physical trespass analysis in *Jones*. In that case, law enforcement officers installed a GPS tracking device on an individual's vehicle and subsequently used that device to monitor the vehicle's movements on public streets. The Court applied trespass principle here instead of the reasonable expectation of privacy test, reasoning that the officers had physically intruded into the defendant's constitutionally protected privacy rights. A concurring opinion by Justice Alito declined to take that approach, instead applying the *Katz* test and suggesting that the "relatively short-term monitoring of a person's movements on public streets" was ok, but "the use of longer term GPS monitoring in investigations of most offenses" might violate the Fourth Amendment in the absence

<sup>93</sup> Kyllo v. United States, 533 U.S. 27. (2001).

<sup>&</sup>lt;sup>94</sup> Stephen E. Henderson, Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search, 56 MERCER L. REV. 507, 562 (2005).

of a search warrant.95

Justice Alito realizes the challenges caused by emerging new surveillance technologies may invade privacy much more severely than before. "In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical."<sup>96</sup> The resources required impeded the outrageous use of the monitoring methods. But the "devices like the one used in the present case . . . make long-term monitoring relatively easy and cheap."<sup>97</sup>

It is understandable that the Court in *Jones* hesitated to rush to resolve this novel question. As Justice Alito explained, "the best that we can do in this case is to apply existing Fourth Amendment doctrine."<sup>98</sup> Tellingly, however, he also suggested that the judiciary might have only a limited role to play in regulating video surveillance: "In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative."<sup>99</sup>

## FOIA

Despite falling outside the protection of privacy under the Fourth Amendment, people who value their privacy may have another federal option: requesting that the government disclose information under the Freedom of Information Act (FOIA). Public access to the contents of individual information captured by the surveillance systems would be controversial, and might itself violate privacy rights,<sup>100</sup> or might allow criminals to take advantage of the information. Nonetheless, FOIA disclosure can bring the kind of transparency that democracy needs to oversee government acts.

<sup>&</sup>lt;sup>99</sup> See Jones, 132 S. Ct. at 954.

<sup>&</sup>lt;sup>96</sup> Id. at 964.

<sup>&</sup>lt;sup>97</sup> Id.

<sup>&</sup>lt;sup>98</sup> Id.

<sup>&</sup>lt;sup>99</sup> Id.

<sup>&</sup>lt;sup>100</sup> Newell, *supra* note 83.

Knowing how the police department implements the video surveillance system is vital to the public interest because classified methods may be illegal. In addition, potential abuse of this system will invade everyone's privacy. However, as a result of a tangled understanding of FOIA, at present the public's desire to know the watcher behind the cameras is not satisfied.

A notable example comes from the NYCLU. In 2007, the organization filed requests with the NYPD and the Department of Homeland Security (DHS) under FOIL and FOIA, trying to discover how the City's video surveillance system was being implemented and operated. The NYCLU's goal was to draw a picture for the public.<sup>101</sup> The response from the NYPD to the request was to provide merely one document. The NYPD asserted that the rest of documents sought "were either exempt from disclosure or could not be located."<sup>102</sup>Although additional documents were disclosed after an administrative appeal, most were just budgetary worksheets and funding requests.<sup>103</sup>

In the federal court, the defendant was the DHS, from which the NYPD received grant funding. Documents at issue were mainly about the location of cameras, the types of equipment used and the implementing timeline of the New York video surveillance system. The government relied principally on FOIA Exemption 7(E), which applies to

[R]ecords or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information ... would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law.<sup>104</sup>

The police department was afraid that potential criminals could take advantage of the information, thereby facilitating "circumvention of the law."

<sup>103</sup> Id.

<sup>&</sup>lt;sup>101</sup> New York Civil Liberties Union v. Dep't of Homeland Sec., 771 F. Supp. 2d 289, 290 (S.D.N.Y. 2011)

<sup>&</sup>lt;sup>102</sup> Greer, *supra* note 62, at 600. (citing New York Civil Liberties Union v. Dep't of Homeland Sec., 771 F. Supp. 2d 289, 290 (S.D.N.Y. 2011).)

<sup>&</sup>lt;sup>104</sup> 5 U.S.C. § 552(b) (7).

Because the court agreed that the generally known routine technologies and procedures were not under Exemption 7(E), the key issue was whether the information the plaintiff requested was "identical" to the publicly available information. The district court held that the request was not identical to information publicly available, and therefore, allowed the police's refusal to disclose documents under the exemption.<sup>105</sup> The court noted that the public did not know specific locations of cameras and license plate readers used in the initiative, not to mention methods of data transmitting. It agreed with the government that such information could be used to circumvent the law.<sup>106</sup> After argument, DHS withdrew its claim that the total number of cameras and license plate readers used or planned for the surveillance system were also exempt from disclosure. Yet even after that information was no longer at issue in the case, NYPD still refused to disclose that information.<sup>107</sup>

Under analysis, the "identical" requirement is an extremely high standard. If the government had not initially released the information before the FOIA request, it would be very hard to prove the public available information is identical to the inside government information. Although there are possibilities that information could be released by an informant, it is unlikely that the public can rely on a Deep Throat or other whistleblower. Thus, after the case, it is much harder for the public in New York to know the whole picture of the video surveillance system, as long as the court relies on "the identical to public availability" doctrine to justify the refusal to disclose information. Meanwhile, the incentive of initial reveals by the government decreased. The reason is simple: the government does not want the initially released information come back to haunt it.

A similar result occurred in Chicago, according to a study "Chicago's Video Surveillance

<sup>&</sup>lt;sup>105</sup> 5 U.S.C.A. § 552(b)(7).

<sup>&</sup>lt;sup>106</sup> New York Civil Liberties Union v. Dep't of Homeland Sec., 771 F. Supp. 2d, at 291.

<sup>&</sup>lt;sup>107</sup> Def.'s Ltr. of Mar. 3, 2011, at 1, New York Civil Liberties Union v. Dep't of Homeland Sec., 771 F. Supp. 2d 289, 291 (S.D.N.Y. 2011).

Cameras: A Pervasive and Poorly Regulated Threat to Our Privacy":

When the ACLU sent a Freedom of Information Act (FOIA) request to the City regarding its camera system, the City refused to state whether there had been any alleged misuse of the cameras, and did not disclose any electronic data regarding the cameras' alleged effectiveness. Likewise, there was no public information available regarding the total number of cameras, the location of most cameras, the total amount of money spent on the cameras, and the sources of that money. Moreover, the City repeatedly failed to respond to the ACLU's requests for permission to visit the OEMC's operations center, and repeatedly failed to respond to the ACLU's letters proposing new regulations.<sup>108</sup>

# **B.** Self-restraint by the Executive Branch

Despite silence from the judicial branch, the U.S. government does not operate in vacuum. Some degree of self-restraint still exists in implementing and operating video surveillance systems. But existing self-restraint regulation has more symbolic meaning than operational meaning. Its inherent deficiency is that it is far from adequate to protect people's privacy rights. An analysis of NYPD guidelines echoes the previous concerns expressed by two scholars, Clive Norris and Gary Armstrong, who found that many codes of practices in Britain contained "fine sounding rhetoric" about the importance of individual privacy, but provided little in the way of actual protection against intrusive or unwanted surveillance due to the lack of detail and definition regarding core procedures.<sup>109</sup>

#### **Intra-department Guidelines**

In 2009, the NYPD published its "Public Security Privacy Guidelines" to establish policies and procedures to limit the authorized use of the Domain Awareness System and to provide for limited access to and proper disposition of stored data.<sup>110</sup> According to the guidelines, the Domain

<sup>&</sup>lt;sup>108</sup> Schwartz, *supra* note 6, at 54.

<sup>&</sup>lt;sup>109</sup> Goold B J, CCTV and Policing: Public area surveillance and Police Practices in Britain. Oxford University Press 100 (2004).

<sup>&</sup>lt;sup>110</sup> New York City, N.Y., N.Y.C. Police Dep't Pub. Sec. Privacy Guidelines (Apr. 2, 2009), [hereinafter, NYC

Awareness System is technology deployed in public spaces as part of the counterterrorism program of the NYPD's Counterterrorism Bureau, including: NYPD-owned and Stakeholder-owned CCTV providing feeds into the Lower Manhattan Security Coordination Center; License Plate Readers; and other domain awareness devices, as appropriate.<sup>111</sup>

By the statement of purpose, the Domain Awareness System is designed as a counterterrorism

tool:

Facilitate the observation of pre-operational activity by terrorist organizations or their agents, detect and deter terrorists' attacks, provide a degree of common domain awareness for all Stakeholders, reduce incident response times, and create a common technological infrastructure to support the integration of new security technology.<sup>112</sup>

In response to privacy concerns, the guidelines announce that:

[N]o person will be targeted or monitored by the Domain Awareness System solely because of actual or perceived race, color, religion or creed, age, national origin, alienage, citizenship status, gender (including gender identity), sexual orientation, disability, marital status, partnership status, military status, or political affiliation or beliefs.<sup>113</sup>

The guidelines further state that the system will be used only to monitor public areas and public activities, and that the powerfully intrusive facial recognition technology will not be utilized. The guidelines set a Pre-Archival Period for Video of 30 days. After that, the data must be destroyed unless retention approved by the Authorized Agent. And for data use, intra-approval procedures are listed.<sup>114</sup> In addition, the guidelines make clear that all personnel access to the system will complete privacy training.<sup>115</sup>

guidelines], http://prtl-prd-web.nyc.gov/html/nypd/downloads/pdf/crime\_prevention/public\_security\_privacy\_ guidelines.pdf.

 $<sup>\</sup>overline{111}$  Id.

<sup>&</sup>lt;sup>112</sup> *Id*.

<sup>&</sup>lt;sup>113</sup> Id.

<sup>&</sup>lt;sup>114</sup> Id.

<sup>&</sup>lt;sup>115</sup> Id.

#### Lack of Constraint

Although addressing some concerns, basically, the guidelines are a rough outline. A few key issues are ignored or avoided. Because even with clear rules and procedures in place, horrendous privacy violations can and do occur, as previously discussed,<sup>116</sup> it is hard to count on these outlines to protect privacy.

(1) Law enforcement purpose

From the beginning, the Domain Awareness System was designed for counterterrorism purposes, as the guidelines clearly state. But law enforcement is another use of this system, even though not listed in the primary purpose. Whereas anti-terrorism efforts involve high interests of the national security, law enforcement efforts are more ordinary and much easier to confront with the citizens' daily life, especially after the 9/11 attacks. Since people's privacy is susceptible to the video surveillance used for law enforcement purpose, there should be clear regulations designed for this purpose.

But there is no such limitation in the guidelines. Under the column "data usage," the guidelines state that "in limited circumstances, data from the Domain Awareness System may also be used in furtherance of legitimate law enforcement and public safety purposes beyond the scope of those purposes set out in the Statement of Purpose (III.B)."<sup>117</sup> It is unclear what "the limited circumstances" are. In addition, the "individual seeking to make the secondary use of data must have a reason to believe the data will further a law enforcement or public safety purpose."<sup>118</sup> But "a reason to believe" is mere a relevance standard, which means any reason is ok, no matter how attenuated it may be. This requirement is too vague to guide the officer's discretion or to provide

<sup>&</sup>lt;sup>116</sup> Siegel, *supra* note 33.

<sup>&</sup>lt;sup>117</sup> Id.

<sup>&</sup>lt;sup>118</sup> Id.

meaningful line on which the intra-department authorized agent to decide. In addition, there is no provision for outside review of the justification for the officer's decision.

## (2) Incidental use

The incidental use of the system needs no additional approval. If the user who applies the system in furtherance of counterterrorism purpose incidentally notices something useful for a legitimate law enforcement or public safety, no approval is needed, meaning that when someone is sitting behind the cameras, there are no limits on the purposes for which he can use this powerful system. The inherent possibility of abuse is not merely imaginary. Practices in other cities, discussed above, make clear that the power behind the cameras is susceptible to abuse. For instance, operators in Chicago have power to use video surveillance cameras to aim at particular members of the public, and to zoom in to see small objects at great distances. This power cannot be observed by ordinary people, let alone be overseen by them.<sup>119</sup>

Moreover, if the incidental use needs some exploration into the database to get some comparative results, does the operator needs approval to do that? According to the incidental use policy that the officers have to response quickly to the situation they observed, it is safe to make an assumption that no approval is needed under that circumstance. Thus, the access to the database under such circumstance is unfettered.

## (3)Internal norms

There are some internal norms, but those restrictions are effectively toothless. For instance, the secondary use of the data from the system has to be approved by an authorized inside agent, if it is intentionally used for a legitimate law enforcement or public safety purpose. The authorized agents, however, are the Deputy Commissioner of Counterterrorism and the Deputy Commissioner

<sup>&</sup>lt;sup>119</sup> Schwartz, *supra* note 6, at 57.

for Legal Matters—both inside the police department. Moreover, as the last provision of the guidelines makes clear, "Nothing in these Guidelines is intended to create any private rights, privileges, benefits or causes of action in law or equity."<sup>120</sup> Thus, no doubt are the guidelines just the internal norms, rather than having concrete legal consequences.

# C. Legislation at the National, State, and Local Level

In *Jones*, Justice Alito thought new intrusions on privacy might spur the enactment of legislation to protect against these intrusions. He saw this as what ultimately happened with respect to wiretapping. After *Katz*, Congress did not leave it to the courts to develop a body of Fourth Amendment case law governing that complex subject. Instead, Congress promptly enacted a comprehensive statute, see 18 U.S.C. §§ 2510–2522 (2006 ed. and Supp. IV), and since that time, the regulation of wiretapping has been governed primarily by statute and not by case law. <sup>121</sup>

Justice Alito's opinion reflects the general attitude from the judicial branch and indicates that the breakthrough in the privacy issue raised by the video surveillance might lie in the legislative branch. In practice, however, the opposite may be true. A recent survey shows that with few exceptions "the use of facial recognition and video surveillance remains surprisingly unregulated."<sup>122</sup> As an exceptional example, the State of Virginia House of Delegates passed a bill that requires law enforcement to get judicial approval before installing facial scanning technology, limiting the technologies use to situations where it is likely to provide information about a felony. The Virginia bill also bars law enforcement from retaining a person's image in a database unless the facial recognition software matched her to a potential crime.<sup>123</sup>

<sup>&</sup>lt;sup>120</sup> NYC guidelines, *supra* note 110.

<sup>&</sup>lt;sup>121</sup> United States v. Jones, 132 S. Ct. 945, 962, 181 L. Ed. 2d 911 (2012).

<sup>&</sup>lt;sup>122</sup> Stephen Rushin, *The Judicial Response to Mass Police Surveillance*, U. ILL. J.L. TECH. & POL'Y, 281,289 (2011). <sup>123</sup> *Id*.

Contrary to the Virginia "notable exception," however, the sequence of events in Chicago is more common. The ACLU advocated for a bill that would have required every government agency that operates or has access to public surveillance cameras to annually disclose their total number of cameras, along with any camera privacy policies. But the bill failed to pass. Indeed, in 2012, an ordinance allowed the Mayor of Chicago to purchase and deploy new surveillance cameras without any approval from, or even notice to, the City Council.<sup>124</sup> That experience is typical. A 2006 study found that only 8 percent of jurisdictions operating video surveillance systems had enacted legislation to regulate the systems' operation and use.<sup>125</sup>

# **D.** Obstacles to Meaningful Regulation of Video Surveillance

#### Lack of public debate

In the progress of legislation, the power of public opinion plays an important role in a democratic system. If the public has no opportunity to fully discuss issues involving peoples' lives, and to register their concerns and advocate some restraints on the use of power by the government, quickly developed technology can endanger people's rights.

The reality shows that valuable public participation in public video surveillance implementation is absent in the United States. In 2005, Thomas J. Nestel, the Philadelphia Police Staff Inspector, surveyed police departments in fifty largest U.S. cities, requesting from each its policy and practice guidelines for video surveillance cameras. His study expressed concern that the community was not involved in the initial or subsequent implementation process.<sup>126</sup>

<sup>&</sup>lt;sup>124</sup> Schwartz, *supra* note 6, at 54.

<sup>&</sup>lt;sup>125</sup> See Thomas J. Nestel, III, *Using Surveillance Cameras to Monitor Public Domains: Can Abuse Be Prevented?* (March 2006) (unpublished M.A. dissertation, Naval Postgraduate School) available at

https://www.hsdl.org/homesec/docs/theses/06Mar\_Nestel.pdf&code=c652f57a750279b26159c07bb6989fd6. <sup>126</sup> Siegel, *supra* note 33.

Absence of public participation in the legislation partly lies in the fact that the public has limited information about the video surveillance system and the potential threat this powerful system can cause. It also lies partly in the secret nature of the video surveillance system itself, which means the people cannot easily become aware of the abuse of the surveillance power or bring individual lawsuits for the infringement of privacy rights.

First, lack of information is the direct result from police departments' refusal to disclose information. One scholar has identified two barriers to discussion, debate, and enforcement of video surveillance regulations in New York. One is the NYPD's court-supported refusal to release the majority of documents related to the operations of video surveillance programs. The other is the unenforceable nature of the NYPD's Public Security Privacy Guidelines.<sup>127</sup>

Second, the individual is hard to detect this privacy invasion by cameras. If no requirement on the government to disclose information initially, the abuses will go unnoticed since the individual will not be sufficiently informed and empowered to challenge them.<sup>128</sup>

## The interest of the industry

When careful policymakers want to make a decision, they should know whether this policy is cost-effective. Considerable research has raised concerns about the cost-effectiveness of video surveillance.<sup>129</sup> In Britain, a number of local authorities have yearly operating budgets of over \$500,000 for camera systems that cover downtown areas.<sup>130</sup> The annual budget of each of the several 100-camera systems in New York City housing projects is approximately \$850,000 just for

<sup>&</sup>lt;sup>127</sup> Greer, *supra* note 62, at 615.

<sup>&</sup>lt;sup>128</sup> Id. at 626.

<sup>&</sup>lt;sup>129</sup> Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 231-32 (2002).

<sup>&</sup>lt;sup>130</sup> G. Wade, Funding CCTV: The Story So Far, 7 CCTV TODAY 28 (1998).

staffing (i.e., not including the upfront costs of the cameras, the maintenance, new tapes, tape storage, and associated expenditures). <sup>131</sup> Those figures raise the question whether other alternatives, such as more patrols, better lighting and greater community participation in law enforcement, could achieve equal or better results at less cost. The studies that have examined the impact of video systems have found the systems to have less effect on crime than alternative policing methods--like more beat officers or street lighting--that would cost the same amount of money.<sup>132</sup>

That kind of cost-benefit analysis, especially the consideration of alternatives to replace video surveillance, would probably make the mass surveillance industry in panic. The industry is a multibillion dollar business that has experienced phenomenal growth rates since 2001. According to data provided by *The Wall Street Journal*, the retail market of surveillance tools has sprung up from "nearly zero" in 2001 to about US\$5 billion in 2011.<sup>133</sup> The size of the video surveillance market has risen from \$11.5 billion in 2008 to \$37.5 billion in 2015.<sup>134</sup> Some views that disregarding the cost-benefit analysis can support that implementation are the promotor of this giant industry. "In tragedy's aftermath, it can be tough to have a serious conversation about how much to invest. But when the goal is to push risk as close to zero as possible, spending can asymptotically stretch into infinity."<sup>135</sup>

Industry self-interest might be an important part of the story behind the tepid response to video surveillance from the legislative process. The legislative process is not merely a forum for

<sup>131</sup> See generally Remarks of Thomas Coty (Manager of the National Institute of Justice Video Sensor and Processing Program), at Meeting of the Security Industry Association and International Association of Chiefs of Police, at 22(Apr. 17, 2002) (transcript available at http:// www.securitygateway.com/E/E3\_5.html).

<sup>&</sup>lt;sup>132</sup> Jeremy Brown, *Pan, Tilt, Zoom: Regulating the Use of Video Surveillance of Public Places*, 23 BERKELEY TECH. L.J. 755, 773-74 (2008).

 <sup>&</sup>lt;sup>133</sup> Jennifer Valentino-Devries, *Document Trove Exposes Surveillance Methods*, WALL ST. J., Nov. 19, 2011, http://www.wsj.com/articles/SB10001424052970203611404577044192607407780.
<sup>134</sup> Proctor, *supra* note 5.

<sup>&</sup>lt;sup>135</sup> Id.

the protection of civil rights, but also a place where the businessmen try to influence in order to acquire or keep their interests. When the voice advocating for public civil rights is relatively quiet, no competing force in the legislation can counter a giant industry that benefits from the boom in video surveillance implementation. After all, the natural attitude of the industry is to resist any discussion or regulation on the implementation of video surveillance.

# Public safety perspective

Putting aside insufficient public attention and the interests of industry, one crucial reason that legislatures have been reluctant to limit video surveillance systems is concern about national security and public safety.

After the September 11 attacks, the trend of using surveillance technologies has increased rapidly. Although controversial,<sup>136</sup> the common view of these technologies is that they make society safer by deterring and preventing terrorist attacks and crimes.

The extent to which such measures do anything to protect from further tragedies is questionable, but largely irrelevant. For politicians, there is a need to be seen to be doing something. And as the psychological, social or political conditions that give rise to such incidents are complex, and possibly intractable, technological fixes which promise the appearance, if not the reality of security are highly appealing. When such crises occur, funding will be made available, more sober judgements as to effectiveness and alternatives ignored, and legal restrictions and constitutional objections set aside, as it will be argued that the balance between civil liberties and security will have to be tilted in favor of security.<sup>137</sup>

This expansion has lasted for 14 years. Now, the unification of diverse data sources, such as video surveillance cameras linked with centralized facial image databases and facial recognition software, digital identification based on fingerprints, retinal scans, and voice patterns, automobile

<sup>&</sup>lt;sup>136</sup> *Id.* (What we saw in Boston largely confirmed what we already knew," said Ben Wizner, Director of the ACLU's Speech, Privacy & Technology Project. "Cameras are ineffective at the prevention and deterrence of serious crime. They can be very effective at solving crime." But advocates of surveillance point to advancements in technology as proof that cameras will, in the future, enhance response and assist prevention.)

<sup>&</sup>lt;sup>137</sup> Norris, *supra* note 60, at 126.

tracking devices and tracking of cell phone data, is under way. These powerful systems could become a centralized repository accessible to all governmental agencies and make watchers always know who, and where, individuals are.<sup>138</sup> As an indivisible part of this system, there is no doubt that the video surveillance is a powerful law enforcement tool hard to discard.

To summarize, despite many years of requests for regulations, the reality has not actively responded to the theory. Three branches' responses to the video surveillance system discussed in this part demonstrate that the privacy issue has become deadlocked due to the interacting effects three branches place on each other:

- The Supreme Court recognizes the privacy challenges raised by pervasive monitoring systems, but has insisted that the proper solution might be legislative.
- Under existing statutes, police and other executive agencies are exempt from disclosing most of the information about the video surveillance system.
- Due to the lack of disclosure, the public lacks complete information about the implementation of the video surveillance system and public discussion becomes inadequate.
- Unawareness of the invasion of privacy makes it difficult for the public to take individual judicial action.
- Lack of public debate has a negative effect on the legislative process.
- As a consequence, no legislative regulation of the police can emerge, leaving only weak self-restraint norms to prevent abuses.

<sup>&</sup>lt;sup>138</sup> Miller, supra note 17, at 111.

# **III.** Strengths and Limits of the Judicial and Legislative Branches

Having identified a deadlock in the responses of each branch of government to the challenges of public video surveillance, several questions are left open. Does the structure of the government itself give rise to this deadlock? More importantly, where is the weak point in this deadlock the privacy advocates could break through? The courts? Legislatures? The self-regulation practices of police departments? Or the public?

As Dr. William Webster has proposed, a policy perspective might be more likely to offer a comprehensive explanation for the CCTV revolution or the ongoing support for CCTV technologies. The policy perspective

highlights the complex intertwined interactions between government, policymakers, the media, service providers and users, and technological and policy developments. Such an approach stresses the power relations and social interactions between different actors and institutions in the governance and public policy process and points to CCTV as an important social and policy construct and not just a technological artifact.<sup>139</sup>

Similarly, the following two parts will take the policy perspective to explore what three branches of the government can and cannot do if they want to seriously regulate public video surveillance, based on their positions and roles in the political structure. They do so by drawing comparisons with Britain and China, and by considering how the Separation of Powers and Federalism deeply rooted in the United States political system might be crucial factors that lead the U.S. public video surveillance regulation practice to a different path.

# **A. Judicial Branch**

## The position to set a uniform standard

<sup>&</sup>lt;sup>139</sup> Webster CWR, CCTV policy in the UK: Reconsidering the evidence base, 6 (1) SURVEILLANCE & SOC'Y, 10 (2009).

In a federal system like the United States, obviously, the easiest way for the whole country to adapt a new uniform standard of regulation is an opinion of the Supreme Court on a constitutional issue. The Court is structurally positioned in the decentralized federal system to address national concern about public video surveillance. But the opinions the Court has given, which focus mainly on the reasonable expectation of privacy or trespass, have not proven as helpful in regulating video surveillance as other kinds of surveillance.

In the past decades, the Supreme Court has succeeded in resolving some issues in the surveillance area under the Fourth Amendment clause. With respect to wiretapping, the Supreme Court in *Katz* ruled that the surveillance technique employed to a public booth constituted a Fourth Amendment search because it violated a reasonable expectation of privacy.

Two particular features of public video surveillance, however, have complicated efforts to bring such systems under the Fourth Amendment. First, video surveillance has surface-bound nature which does not dig into the concealed things in human bodies, and it occurs in public places, where people have no expectation of privacy under *Katz*. Thus, Fourth Amendment jurisprudence has differentiated video surveillance from other forms of monitoring by holding that it is not a search at all. Second, even if public video surveillance is a search, it might be a "reasonable" search if anti-terrorism is involved. As a result, pervasive public video surveillance remains unconstrained by the Fourth Amendment.<sup>140</sup>

Of the various facets of the privacy threatened by public video surveillance, the most frequently discussed is information privacy. But the logic of *Katz* leads to a dead end. People in public places have no reasonable expectation of privacy is a crystal doctrine. Period.

The most coherent and elaborate repertoire of rules and techniques is concerned with the protection of personal information, rather than personal movement, physical presence in certain kinds of space, or bodily integrity as such, although these too are involved in the

<sup>&</sup>lt;sup>140</sup> Blitz, *supra* note 86, at 1359.

processing of information and personal data and to that extent remain governable by legacy regulatory systems. <sup>141</sup>

However, information privacy is just one crucial part of issue in the video surveillance area, not the whole story. Unfortunately, the Supreme Court has not given a clear opinion on the other facet of video surveillance-the pervasive suspicionless recording of people's everyday public lives. Katz and its progeny focus entirely on different sort of threats from surveillance, and do not address anything as to the pervasive recording facet of public surveillance systems. Meanwhile, the rule in Katz has limited the Court's ability to address that facet in future cases. According to Professor Marc Jonathan Blitz, the Supreme Court was stuck with the Katz test. Although Katz's goal was to extend Fourth Amendment privacy rights beyond those traditional privacy zones (most notably the home), Justice Harlan's concurring opinion led the Court into a narrower rule. The reasonable expectation of privacy "appears to focus less on a person's actions and more on the place in which he acts,"<sup>142</sup> which is on the opposite of the Court's majority opinion, holding that the Fourth Amendment protects people, not places. This protection idea focusing on people could have been "made portable and taken with people as they traveled from place to place." <sup>143</sup> In Professor Blitz's view, "Justice Stewart's majority opinion may bear as much as responsibility as Harlan's concurrence for the failure to extend constitutional privacy protections to public spaces"<sup>144</sup> because it did not provide guidance as to when activities in public should count as private. "Its failure to provide any such limiting principle left future courts nothing to rely upon except the familiar distinction between private and public areas."<sup>145</sup>

<sup>&</sup>lt;sup>141</sup> Wood D M, Ball K, Lyon D, et al., *A report on the surveillance society*, Survillance Studies Network, 89, (2006). (U.K.), https://ico.org.uk/media/about-the-ico/documents/1042388/surveillance-society-public-discussion-document-06.pdf.

<sup>&</sup>lt;sup>142</sup> United States v. Taborda, 635 F.2d 131(2d Cir. 1980).

<sup>&</sup>lt;sup>143</sup> Blitz, *supra* note 86, at 1359.

<sup>&</sup>lt;sup>144</sup> Id.

<sup>&</sup>lt;sup>145</sup> *Id*.

The growing power of public video surveillance is rooted in massive and integrated systems. They are totally different from the decades-old practice of pointing a camera at someone. But the Supreme Court has been nonchalant in responding to this dramatic change. It has acted "as though these novel and far-reaching technological developments are not really novel at all— but rather more effective and cost-efficient variants of long-accepted methods of police work."<sup>146</sup> Most surprisingly, in *Jones*, the Court even returned to the trespass test to supplement the reasonable expectation of privacy test. From any perspective, it looks like the Court picked up the easiest way to close the case, trying to avoid solving the real thorny problem.

Obviously, silence from the Court does not necessarily mean that the Court has not realized the challenge posed by pervasive public video surveillance systems. Case law from around the nation reveals some attitudes in the judicial branch. Some courts have tried to expand the category of "private" environments in public places, holding for example that stores and workplaces qualify as "private" environments.<sup>147</sup> Although "no general privacy interest" exists in these places, being videotaped in them is still forbidden because people may have expectation of privacy. Other courts have doubted that public video surveillance can remain shielded from Fourth Amendment scrutiny, basing on the reason as to the mass nature of the systems.<sup>148</sup> The scale of the surveillance and the degree to which it is constrained may determine the result whether it triggers the Fourth Amendment or not. The clearest assertion was in *Jones*, where Justice Alito in his concurrence stated: "[r]elatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable. But the use of longer term

<sup>&</sup>lt;sup>146</sup> *Id*.

<sup>&</sup>lt;sup>147</sup> See, e.g., United States v. Taketa, 923 F. 2d 665, 677 (9<sup>th</sup> Cir. 1991); State v. Thomas, 642 N.E.2d 240, 246(Ind.

Ct. App. 1994); State v. Bonnell, 856 P.2d 1265, 1277(Haw. 1993).

<sup>&</sup>lt;sup>148</sup> E.g. State v. Costin, 720 A.2d 866 (Vt. 1998); Cowles v. State, 23 P.3d 1168, 1171 (Alaska 2001).

GPS monitoring in investigations of most offenses impinges on expectations of privacy."149

# Discussion

After decades of discussion, however, the Court in *Jones* ducked the chance to address the constitutionality of public monitoring, resolving a challenge to GPS tracking on narrow trespass ground rather than setting up new rules, even as it recognized the new threats from the emerging video surveillance in public places. Several reasons may explain the Court's reluctance.

First, modifying Fourth Amendment jurisprudence as to privacy rights in public places would require the reconsideration and perhaps overruling of considerable Supreme Court precedent, which is entitled to respect under *stare decisis*. Since *Katz* has established a narrower rule and left little room to protect the privacy of public places, the Court was stuck into it to some extent. On the other hand, Professor Stuart M. Benjamin has pointed out that "Rapidly changing facts weaken the force of *stare decisis* by undermining the stability of precedents."<sup>150</sup>

Second, once the Court concludes that the pervasive recording of people's public lives might violate the Constitution, the first question it must answer is how to draw a line between pervasive recordings and a permitted video surveillance. Any movement towards the direction that the pervasive recording is unconstitutional may lead to a conclusion that all public video surveillance systems should be forbidden. It is quite clear the Court does not want to step into that extreme and awkward position.

Third, the Court might not be in better position than the legislature when new technologies are involved. Justice Alito stated: "In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative."<sup>151</sup> When facing the new development of

<sup>&</sup>lt;sup>149</sup> United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring).

<sup>&</sup>lt;sup>150</sup> Stuart Minor Benjamin, *Stepping into the Same River Twice: Rapidly Changing Facts and the Appellate Process*, 78 TEX. L. REV. 269, 272 (1999).

<sup>&</sup>lt;sup>151</sup> Id.

technologies, the Court is likely to try to catch up with it but could always be left behind. The facts in the prior cases may not reflects the recent changes in the later ones. And compared with the legislature, the judicial branch has less physical and administrative resources and is less technologically sophisticated.<sup>152</sup>Moreover, because public video surveillance systems are used by the executive branch as anti-terrorism and law enforcement tools, it is predictable that the Court will be deferential to the decisions made by the executive branch.

In sum, although the Supreme Court is in a strong position to address the public video surveillance issue in a national and uniform manner, there is little hope at present that society will get clear guidance from the judicial branch on this matter. Because the new challenges brought by these emerging technologies require a breakthrough in the Fourth Amendment jurisprudence, and it will be hard for the Court to draw a line between constitutional and unconstitutional of public video surveillance without placing grave burdens on law enforcement. The Court is therefore likely to await a response from the legislative process first.

# **B.** Legislative Branch

This part will draw upon the experience of legislative limits on public video surveillance in Britain and compare it with its counterparts in the United States.

### **Legislation in Britain**

The use of CCTV systems in Britain remained unregulated for a long time, until the end of 1990s. Around that time, however, several acts of Parliament included elements regulating CCTV. In 1998, the Human Rights Act was enacted to incorporate into UK law the rights contained in the European Convention on Human Rights. The Act made a remedy for breach of a Convention

<sup>&</sup>lt;sup>152</sup> Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 875-77 (2003-2004).

right available in UK courts, without the need to go to the European Court of Human Rights. Thus, the protection of privacy was set up in the statute.

The Data Protection Act of 1998 (DPA) is the main piece of legislation that governs the protection of personal data in Britain. Although the Act itself does not mention privacy, it was enacted to bring British law into line with the EU data protection directive of 1995 which required Member States to protect people's fundamental rights and freedoms and their right to privacy with respect to the processing of personal data in particular. It required that the installation and operation of CCTV systems should comply with a specific legal basis, such as prevention and detection of crime, apprehension and prosecuting the offenders or public/employee safety.<sup>153</sup> It also set up a registration requirement for surveillance systems.<sup>154</sup> But critics charged that those acts were not adequate for the privacy protection from the CCTV intrusion: "Both the new Data Protection and Human Rights Acts have been toothless to prevent the expansion of CCTV and very weak at regulating it once in place."<sup>155</sup>

The more important acts were the Regulation of Investigatory Powers Act (RIPA) and the CCTV Codes of Practice, both enacted in 2000. The RIPA aims at making investigatory powers used in accordance with human rights. One part is specifically designed to regulate the overt surveillance activities of public authorities. Police and other agencies who use overt surveillance have to follow the principles of proportionality, legality, accountability, necessity and subsidiarity.<sup>156</sup> RIPA also establishes an Investigatory Powers Tribunal to hear complaints about surveillance by public bodies. Offenses involving the abuse of investigatory powers can be

<sup>&</sup>lt;sup>153</sup> McCahill, *supra* note 20, at 52.

<sup>&</sup>lt;sup>154</sup> Marianne L. Gras, *The Legal Regulation of CCTV in Europe*, SURVEILLANCE & SOC'Y 217 (2004), http://www.surveillance-and-society.org/articles2(2)/regulation.pdf

<sup>&</sup>lt;sup>155</sup> Norris, *supra* note 60, at 121.

<sup>&</sup>lt;sup>156</sup> McCahill, *supra* note 20, at 51.

prosecuted.

The CCTV Codes of Practice were published by the information commissioner under the DPA to provide detailed advice and guidance in applying the data protection principles in operating the CCTV systems. This code was updated once in 2008 before the passing of the Protection of Freedoms Act (POFA) of 2012. The latest version of the CCTV Codes of Practice in 2015 "has changed to highlight its focus on the data protection implications of using CCTV and other forms of surveillance cameras."<sup>157</sup>

In 2012, the British government took a significant step to fulfill its commitment to the further regulation of CCTV. The parliament passed the POFA to address public concerns caused by the increasing use and technologically developments of the CCTV. Over the past decade, CCTV has changed, from simply being a camera on top of a pole in the local town center where the images were recorded, to much more sophisticated operations using digital and increasingly portable technology. And more technologies such as Automatic Number Plate Recognition (ANPR) and body worn cameras (BWC) are used commonly by the police. Since "surveillance cameras are no longer a passive technology that only records and retains images, but is now a proactive one that can be used to identify people of interest and keep detailed records of people's activities,"<sup>158</sup> more public concerns are aroused "as to the technology no longer being used solely to keep people and their property safe, but increasingly being used to collect evidence to inform other decisions."<sup>159</sup>

The POFA plays an important role in regulating surveillance systems, the Section 30 of the POFA 2012 has authorized the Secretary of State to issue a new surveillance camera code since

<sup>&</sup>lt;sup>157</sup> ICO, IN THE PICTURE: A DATA PROTECTION CODE OF PRACTICE FOR SURVEILLANCE CAMERAS AND PERSONAL INFORMATION, 2015, at 3 (U.K.), https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf <sup>158</sup> *Id.* 

<sup>&</sup>lt;sup>159</sup> Id.

June 2013 and appointed a Surveillance Camera Commissioner to promote the code and review its operation and impact. The POFA code is also an important document to refer to for issues that go beyond data protection. It addresses issues such as operational requirements, technical standards and the effectiveness of the systems available. It regulates the police, police and crime commissioners and local authorities in England and Wales, along with the National Crime Agency.

All other data controllers are encouraged to follow the POFA code.

As a latest and complete code specified to regulate the video surveillance in public places,

the Surveillance Camera Code of Practice (POFA code) sets out guiding principles designed to:

Provide a framework for operators and users of surveillance camera systems so that there is proportionality and transparency in their use of surveillance, and systems are capable of providing good quality images and other information which are fit for purpose.

Provide information and advice on appropriate and approved operational and technical standards for various aspects of surveillance camera systems and on appropriate and approved occupational and competency standards for persons using these systems or processing images and information obtained by these systems to supplement this code.

Address concerns over the potential for abuse or misuse of surveillance by the state in public places.<sup>160</sup>

The key components of the Surveillance Camera Code of Practice are 12 guiding principles:

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.

2. The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.

3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.

4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.

5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.

6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.

7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted;

<sup>&</sup>lt;sup>160</sup> HOME OFFICE, SURVEILLANCE CAMERA CODE OF PRACTICE, §§ 1.3-1.8 (2013). (U.K.).

the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.

8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.

9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorized access and use.

10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.

11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.

12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.<sup>161</sup>

#### Legislation in the United States

In the United States, by contrast, there is little federal law that specifically applies to video

surveillance in public places.

What Congress treats public video surveillance is entirely different from what it treats electronic surveillance. After *Katz*, Congress followed up and promptly enacted a comprehensive statute, The Wiretap Act. Shortly after, the Court in *United States v. U.S. District Court*,<sup>162</sup> also known as *Keith*, held that court approval was required in order for the domestic surveillance to satisfy the Fourth Amendment. This established the precedent that a warrant needed to be obtained before beginning electronic surveillance even if domestic security issues were involved. In 1978, Congress enacted the Foreign Intelligence Surveillance Act (FISA), prescribes procedures for the physical and electronic surveillance and collection of "foreign intelligence information" between or among "foreign powers."

The Wiretap Act has been amended by Electronic Communications Privacy Act of 1986

<sup>&</sup>lt;sup>161</sup> *Id.* § 2.6.

<sup>&</sup>lt;sup>162</sup> 407 U.S. 297 (1972).

(ECPA). The ECPA extended government restrictions on wiretaps from telephone calls to transmissions of electronic data by computer. Following the 9/11 attacks in 2001, Congress enacted the USA PATRIOT Act of 2001 (Patriot Act). The Patriot Act modified portions of numerous electronic communications laws, including the ECPA and FISA, expanding the authority of federal law enforcement to combat terrorism.

But the ECPA only regulates the surveillance involves a human voice, and the FISA that may regulate all electronic surveillance, including video surveillance, only applies to the "foreign intelligence information" between or among "foreign powers." Thus, video surveillance falls outside the range of either ECPA or FISA.

The prior statutes like ECPA do not cover public video surveillance, fundamentally, because of the novelty of video surveillance and piecemeal implementations. Except some legislative endeavors in state level before 9/11 attacks,<sup>163</sup> only informal guidelines without legal binding effect are published.

Most of those guidelines are provided by professional organizations. The Commission on Accreditation for Law Enforcement Agencies (CALEA) provides a rigorous certification process for the national guidelines, which are published but have no binding legal effect. <sup>164</sup> The Department of Justice has also issued policy guidelines for video surveillance by government agencies. The guidelines note that the existing Federal Wiretap Act (Title III) does not control the use of CCTV systems. They also notes that no than probable cause is needed when search warrants permitting the use of video surveillance are requested.<sup>165</sup> Notably, the guidelines focus primarily

<sup>&</sup>lt;sup>163</sup> At the start of the 2001-2002 fiscal year, a number of states had already drafted or passed surveillance-related legislation. See, Nieto, *supra* note 25.

<sup>&</sup>lt;sup>164</sup> COMMISSION ON ACCREDITATION FOR LAW ENFORCEMENT AGENCIES, THE 5TH EDITION OF CALEA'S STANDARDS FOR LAW ENFORCEMENT AGENCIES MANUAL, 2005.

<sup>&</sup>lt;sup>165</sup> C.R.M. 1-99 § 32, http://www.justice.gov/usam/criminal-resource-manual-32-video-surveillance-use-closed-circuit-television-cctv.

on a single camera which is used to monitor a target rather than pervasive public video surveillance system. The American Bar Association developed a set of standards entitled "Technologically-Assisted Physical Surveillance." The guidance calls for the coordination of law enforcement efforts and collaboration with citizens. It also strongly recommends public meetings and the development of administrative controls and protocols for the storage and release of images.<sup>166</sup>

Standard 2-9.3. Video surveillance

(a) Video surveillance of a private activity or condition is permissible when it complies with provisions applicable to electronic interception of communications [see Standards 2-1.1 et seq. of this Chapter], as modified for video surveillance.

(b) Overt video surveillance for a protracted period not governed by Standard 2-9.3(a) is permissible when:

(i) politically accountable law enforcement official or the relevant politically accountable governmental authority concludes that the surveillance

(A) will not view a private activity or condition; and

(B) will be reasonably likely to achieve a legitimate law enforcement objective; and

(ii) in cases where deterrence rather than investigation is the primary objective, the public to be affected by the surveillance:

(A) is notified of the intended location and general capability of the camera; and

(B) has the opportunity, both prior to the initiation of the surveillance and periodically during it, to express its views of the surveillance and propose changes in its execution, through a hearing or some other appropriate means.

(c) All video surveillance not governed by Standard 2-9.3(a) or (b) is permissible when a supervisory law enforcement official, or the surveilling officer when there are exigent circumstances, concludes that the surveillance:

(i) Will not view a private activity or condition; and

(ii) Will be reasonably likely to achieve a legitimate law enforcement objective.<sup>167</sup>

## Discussion

As an essential element of a free society, privacy is well recognized by the people both in the

United States and Britain. In addition, other commonly known legal, language, and cultural

similarities between Britain and the U.S. make the practice in Britain a good example from which

the United States could learn. As one law student Note has argued:

166

Nestel, supra note 125.

<sup>&</sup>lt;sup>167</sup> AMERICAN BAR ASSOCIATION, CRIMINAL JUSTICE STANDARDS § TECHNOLOGICALLY-ASSISTED PHYSICAL SURVEILLANCE.

http://www.americanbar.org/publications/criminal\_justice\_section\_archive/crimjust\_standards\_taps\_blk.html.

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."<sup>168</sup>

Given those similarities, one might have expected that the United States would follow the road explored by Britain. This part discusses reasons why, to the contrary, the legislative practice in the United States is vastly different from that in Britain.

1. Different political structures and histories of privacy protection

It should not be forgotten that the right to privacy originated in the United States Constitution, while the modern protection of privacy in Britain was just rooted in the European Convention for the Protection of Human Rights and Fundamental Freedoms in 1950.<sup>169</sup> The United States has a longer history of privacy protection than Britain does, and the level of protection is higher where the Constitution is involved. Nonetheless, Britain has developed a system of comprehensive legislation has been enacted to protect privacy over the past two decades, whereas protection in the United States remains inconsistent and segregated. Thus, public video surveillance regulation has been a focus of legislation in Britain, but largely outside the range of U.S. legislatures.

In the United States, the right to privacy was guaranteed by the Bill of Rights and later amendments to the Constitution. It relates to the right of freedom of association, voting rights, protection from unreasonable searches and seizures, and the right of information privacy, including avoiding the disclosure of personal matters, and being independent in decision making.<sup>170</sup> Although the constitutional privacy right protects the individual against the State, state tort law

<sup>&</sup>lt;sup>168</sup> Note, Joyce W. Luk, *Identifying Terrorists: Privacy Rights in the United States and United Kingdom*, 25 HASTINGS INT'L & COMP. L. REV. 223, 256 (2002).

<sup>&</sup>lt;sup>169</sup> Michael W. Heydrich, *A Brave New World: Complying With the European Union Directive on Personal Privacy Through the Power of Contract*, 25 BROOK. J. INT'L L. 407, 417 (1999).

<sup>&</sup>lt;sup>170</sup> PAUL SCHWARTZ & JOEL REIDENBERG, DATA PRIVACY LAW 40-49, (1996).

steps in to protect against the action of other citizens. During the Great Depression, the federal government began implementing increasingly broad legislation, but legislation which touched on the right to privacy could be described as *ad hoc*, targeted at specific government agencies, economic sectors or industries, and often addressed only to narrow and specific issues.<sup>171</sup> Decades later, in an attempt to unify an approach to protecting data, Congress enacted the Privacy Act of 1974,<sup>172</sup> the Computer Matching and Privacy Protection Act of 1988,<sup>173</sup> the Privacy Protection Act of 1980,<sup>174</sup> and the Right to Financial Privacy Act of 1978.<sup>175</sup> But this effort at uniformity failed: "[B]ecause each of these statutes was limited to a specific area or sector, the resulting protection for the individual was neither comprehensive nor consistent."<sup>176</sup>

In the absence of a written constitution, the right to respect for private and family life in Britain was first set out in Article 8 of the Europe Convention on Human Rights. The legislation of privacy protection in Britain was one part of the big picture in Europe. To some extent, Europe's experience in World War II was the hidden agenda behind the European data protection laws, and "the desire to avoid a recurrence of the type of population control exercised by the Nazis and the Gestapo."<sup>177</sup> Then, the advent of technology drove the Council of Europe to begin "to study potential courses for data protection legislation" to prevent privacy rights from being infringed.<sup>178</sup> Once the Council of Ministers of the EU formally adopts a directive, it sets a deadline for member states to transpose the directive to their own law.

Michael W. Heydrich, has sharply argued that, unlike Britain's legislation driven by the

<sup>&</sup>lt;sup>171</sup> FRED H. CATE, PRIVACY IN THE INFORMATION AGE 80 (1997).

<sup>&</sup>lt;sup>172</sup> 5 U.S.C. § 552a (1994).

<sup>&</sup>lt;sup>173</sup> 5 U.S.C. § 552a(o) (1994).

<sup>&</sup>lt;sup>174</sup> 42 U.S.C. § 2000(aa)-(aa)(12) (1994).

<sup>&</sup>lt;sup>175</sup> 12 U.S.C. §§ 3401-3422 (1994).

<sup>&</sup>lt;sup>176</sup> Heydrich, *supra* note 169, at 415.

<sup>&</sup>lt;sup>177</sup> Id. at 417.

<sup>&</sup>lt;sup>178</sup> Peter Mei, The EC Proposed Data Protection Law, 25 LAW & POL'Y INT'L BUS. 305, 307 (1993).

uniform approach adopted by the EU, the United States' use of patchwork of laws leads to inconsistent and inadequate privacy protections:

The European emphasis is on the deterrence of harm and accomplishes this by instituting the necessary control mechanisms for oversight. In contrast, the United States uses a complex patchwork of laws (the Constitution, federal and state legislation, and state common law) to address the right to privacy, taking a reactive stance by legislating in narrow specific areas where problems have occurred. The U.S. emphasis is on use of remedies for damage which has already taken place and prevents future harm by the threat of legal action. This pivotal difference is best explained by providing a general overview of the histories of privacy law in the United States and the countries of the European Union.<sup>179</sup>

According to Heydrich, the difference seems to lie in the different attitudes in controlling video surveillance, the use of prospective legislation in Britain versus the use of retrospective judicial remedies in the United States.

But to read between the lines, it is actually federalism that best explains the difference in the British and U.S. experiences. As is well known, in the United States principles of federalism rooted in historical fear of a strong central government maintain a balance of power between the states and the federal government. When Congress attempts to pass national uniform standards regulating the public video surveillance, federalism operates as an important constraint. Because "[t]he Constitution creates a Federal Government of enumerated powers,"<sup>180</sup> Congress might not directly have authority from the Constitution to create a federal statute to set up a uniform standard of regulating public video surveillance, especially when some systems are operated locally. As a result, the gap in legislation can only be filled by state legislations, informal organization guidelines and so on. "Because of this patchwork method of privacy regulation, the United States may never have an over-arching privacy statute."<sup>181</sup> In contrast, legislation in Britain faces no such

<sup>&</sup>lt;sup>179</sup> Heydrich, *supra* note 169, at 412.

<sup>&</sup>lt;sup>180</sup> United States v. Alfonso D. Lopez, Jr., 514 U.S. 549.

<sup>&</sup>lt;sup>181</sup> Luk, *supra* note 168, at 257.

federalism obstacle, and it is easier to create national-wide regulations. At the same time, the European Union has strongly influenced member states like Britain to accept the uniform standards adopted by the EU.

2. Different attitudes towards the expectation of privacy in public places

In the overview and guiding principle part of the POFA code 2012, the Surveillance Camera Commissioner in Britain declared it is an accepted view that privacy might be interfered by the "modern and forever advancing surveillance camera technology,"<sup>182</sup> because there does exist some expectation of privacy in public places from a developing perspective. The code announced that it "must regulate that potential (to intrude on the right to respect for private and family life), now and in the future."<sup>183</sup>

In considering the potential to interfere with the right to privacy, it is important to take account of the fact that expectations of privacy are both varying and subjective. In general terms, one of the variables is situational, and in a public place there is a zone of interaction with others which may fall within the scope of private life.<sup>184</sup>

This attitude of evolving expectations of privacy has not been affirmed in the United States. Although scholars and judges have long realized that pervasive video surveillance could dramatically transform the expectation of privacy, the Supreme Court has not yet taken a crucial step to close this argument. Some scholars have indicated that the mass surveillance has created a National Surveillance State, in which the focus is on preventing criminality *ex ante*, as opposed to prosecuting crime ex post.<sup>185</sup> Others have warned about mass surveillance and data collection by the state could threaten personal freedom of association and the right to speak anonymously.<sup>186</sup>

<sup>&</sup>lt;sup>182</sup> HOME OFFICE, SURVEILLANCE CAMERA CODE OF PRACTICE § 2.1(2013). (U.K.).

<sup>&</sup>lt;sup>183</sup> *Id.* § 2.3.

<sup>&</sup>lt;sup>184</sup> Id.

 <sup>&</sup>lt;sup>185</sup> Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 3-4 (2008-2009). And Orin S. Kerr, *The National Surveillance State: A Response to Balkin*, 93 MINN. L. REV.2179, 2179 (2009).
<sup>186</sup> E.g., Daniel J. Solove, *Digital Dossier and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1095, 1102 (2002).

Judges have recognized the problem for a relatively long time. In United States v. Garcia,<sup>187</sup> the Seventh Circuit concluded that GPS monitoring of a single suspect without a warrant does not amount to "wholesale surveillance." But Judge Posner quickly followed,

Technological progress poses a threat to privacy by enabling an extent of surveillance that in earlier times would have been prohibitively expensive . . . . Should government someday decide to institute a program of mass surveillance of vehicular movements, it will be time enough to decide whether the Fourth Amendment should be interpreted to treat such surveillance as a search.<sup>188</sup>

Similarly, one year later, in *Jones*, Justice Alito acknowledged "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."<sup>189</sup>

Yet neither the lower federal courts nor the Supreme Court has expanded the scope of the reasonable expectation of privacy doctrine to address the issue involving the jurisprudence of privacy right in public places.

# 3. The effects of 9/11

Another important difference between the British and American experience relates to the 9/11 attacks, and to the timing of efforts to regulate public surveillance. By the end of 1990s, Britain had already adopted a series of privacy and data protection laws prompted by encouragement from the European Union. Had that process continued uninterrupted, the practice in EU might gradually have come influence the U.S. practice under the international "ripple effect" because of the globalization of privacy issues, driven by rising worldwide communication, trade, travel, and marketing activities. In fact, "policy debates in 1997–2000 included sharp discussions of whether the United States should adopt the EU mode."<sup>190</sup>

<sup>&</sup>lt;sup>187</sup> United States v. Garcia, 474 F.3d 994, (7th Cir. 2007).

<sup>188</sup> Id, at 998.

<sup>&</sup>lt;sup>189</sup> United States v. Jones, 132 S. Ct. 945, 964, 181 L. Ed. 2d 911 (2012).

<sup>&</sup>lt;sup>190</sup> Westin, A. F., Social and Political Dimensions of Privacy, 59 J. Soc. ISSUES, 431 (2003).

Indeed, public attention about public surveillance systems had also begun to emerge in the U.S. during the 1990s. Professor Alan Furman Westin has argued that 1990–2002 was "the period when privacy became a first-level social and political issue in the United States."<sup>191</sup> Privacy debates in America during this period responded to several technological developments, such as the rise of the Internet, the arrival of wireless communication devices, the Human Genome Project's unlocking of the genetic code, etc. According to Professor Westin, two of those technologies bore a close relationship with surveillance: "the development of data-mining software based on large data warehousing applications, along with further automation of government public record systems,"<sup>192</sup> and the private use of encryption tools that federal law enforcement and national security agencies sought to block out of concern that "strong encryption programs could immunize online communications by drug dealers and terrorists from lawful surveillance."<sup>193</sup> Those emerging technologies were increasing the public concerns about the privacy.

As Westin explains, there was a stream of more than 120 national surveys in that decade gauging public attitudes toward privacy either wholly or in significant part. He thought those surveys not only raised the public concerns on the privacy, but also resulted in a sound basis for formulating public policies on privacy.

For politicians watching polls and media trends, it was clear by 2000 that championing privacy protection was now very good politics. At the state level, hundreds of new consumer privacy laws were enacted each year in 2000 and 2001, with coalitions of Republican and Democratic political leaders uniting to reflect the privacy concerns of suburbanites, women, Internet users, and other desirable local constituencies.<sup>194</sup>

Suddenly, the attacks of September 11, 2001, drastically changed the privacy protection process. The war against terrorism catalyzed the surveillance expansion. On one hand, public panic

<sup>194</sup> Id.

<sup>&</sup>lt;sup>191</sup> Id.

 $<sup>^{192}</sup>$  Id.

<sup>&</sup>lt;sup>193</sup> Id.

fueled calls for more video cameras on the streets, which is assumed to make the streets safer. A survey done shortly after the 9/11 attack recorded very high public approval of new governmental investigative powers. Among them, up to 86% approved facial-recognition technology to scan for terrorists at public events and places.<sup>195</sup> Although a repeat survey one year later showed that some parts of the high support fell, the support for stronger surveillance and law enforcement measures continues<sup>196</sup>. 58% continued to support extended camera surveillance on streets and in public places.<sup>197</sup> Politicians were happy to oblige by expanding surveillance systems as the public apparently demanded.

# **IV. A Comparative Perspective on the Structure of the Executive**

# **Branch and Regulations of Video Surveillance**

The absence of regulations from the judicial and legislative branches leaves the burden of relieving the tension between security and privacy on the executive branch, especially the police department, the most prominent daily user of public video surveillance. Thus, self-restraint and self-regulations by the executive branch might be the last chance of the government to safeguard privacy interests and remain accountable to the public.

This part primarily compares the U.S. administrative practice with that in China. Those comparisons basing on two pairings of factors: vertical/horizontal and internal/external. By "vertical" and "horizontal," I distinguish between the central government control and the stakeholders' influence at the local level. By "internal" and "external," I distinguish between

<sup>&</sup>lt;sup>195</sup> Harris Interactive & Westin, A. (2001a). *The Harris poll: #49*. New York : Harris Interactive.

<sup>&</sup>lt;sup>196</sup> Harris Interactive & Westin, A. (2002c). *The Harris Poll #46*. New York : Harris Interactive.

<sup>&</sup>lt;sup>197</sup> Westin, *supra* note 204.

effectiveness analysis and the public attitude analysis.

An analysis of those factors leads to the interesting finding that public participation is more necessary in the United States than in China because of different political structures. In an authoritative country, where the executive branch is dominant and local governments are under strict central control and supervision from higher authorities, it does not matter whether governments could get public support on a particular public issue. Administrative regulations could still run smoothly or effectively without adequate public participation. But in a democratic society, public participation is essential not only in justifying particular administrative decisions, but also in keeping the executive branch on the right track.

# A. Administrative Regulations in Different Countries

As discussed above, the global rush to install public video surveillance has been carried out with little systematic attention to the evaluation of those systems,<sup>198</sup> and often with no adequate regulations. Even in systems not subject to meaningful judicial or legislative oversight, however, there are often administrative regulations that govern the operation of the system, and those regulations differ depending on the national context. The basic form of such regulations are guidelines or codes of practice:

Typically, these codes lay down guidelines for the daily operation of the schemes, and cover matters such as staffing, tape handling and storage procedures, security and access to the scheme, and the control and operation of the cameras. Some codes may also include a statement of the purpose and objectives of the scheme, as well as a set of 'rules' designed to protect the public against unwarranted or intrusive surveillance.<sup>199</sup>

In the United States, each police department operating public video surveillance has its own

<sup>&</sup>lt;sup>198</sup> Norris, *supra* note 60, at 125.

<sup>&</sup>lt;sup>199</sup> GOOLD B J., CCTV AND POLICING: PUBLIC AREA SURVEILLANCE AND POLICE PRACTICES IN BRITAIN, 98 2004.

guidelines.<sup>200</sup> These administrative guidelines are different from those informal guidelines published by professional organizations, but obviously the former borrows provisions from the latter. In Britain, apart from the Data Protection Act and other legislative regulations, various administrative regulations limit the use of CCTV, among these, the written codes of practice now widely used by the police.<sup>201</sup> Although a study in 1995 showed "the codes varied considerably in terms of their content, style, and length," considerable efforts have been made by the Home Office and various CCTV user groups to provide some sort of guidance as to best practice, such as "A Watching Brief: A Code of Practice for CCTV" by the Local Government Information Unit in 1996 (LGIU Model), and the Model Code of Practice based on the LGIU model, written by the police and made available to all of the schemes in the Southern Region.<sup>202</sup> In China, The National Development and Reform Commission, Central comprehensive management office, Ministry of industry and information technology, Ministry of public security et al. published "Several Opinions on Increasing Efforts to Establish and Network Public Security Video Surveillance" in May 2015, set up a nationwide goal for the implementation, management and regulations of public video surveillance.

By 2020, will have established and applied networked public video security surveillance, essentially bringing about "full coverage, full network sharing, full-time availability", and achieving visible success in areas such as strengthening public security prevention and control, optimizing transportation, servicing urban management, and innovating social management.<sup>203</sup>

 <sup>&</sup>lt;sup>200</sup> E.g., PITTSBURGH, PA., CODE OF ORDINANCES, § 681.02(e)(i), PRIVACY POLICY FOR PUBLIC SECURITY CAMERA SYSTEMS; D.C., CODE OF MUNICIPAL REG., tit. 24, ch. 25, METROPOLITAN POLICE DEPARTMENT USE OF CLOSED CIRCUIT TELEVISION; SALT LAKE CITY POLICE DEPARTMENT, UTAH, PUBLIC SPACE CAMERAS POLICY (Feb. 18, 2009); DENVER POLICE DEPARTMENT, COLO., OPERATIONS MANUAL, CLOSED CIRCUIT TELEVISION POLICY (revised Jan. 2009); NYPD, N.Y., PUBLIC SECURITY PRIVACY GUIDELINES (effective Apr. 2, 2009).
<sup>201</sup> GOOLD, supra note 199.

<sup>&</sup>lt;sup>202</sup> *Id*, at 99-101.

<sup>&</sup>lt;sup>203</sup> Guanyu Jiaqiang Gonggong Annggon Shipin Jiankong Jianshe Liangwang Yingyong Gongzuo de Ruogan Yijian (关于加强公共安全视频监控建设联网应用工作的若干意见)[Several Opinions on Increasing Efforts to Establish and Network Public Security Video Surveillance], Fa Gai Gao Ji (发改高技) [2015] 996 Hao(号)

Administrative regulations in the operational level can organize and coordinate facilityrelated and human-related aspects of CCTV, which may influence the effectiveness of the system to a great extent.<sup>204</sup> A recent study that analyzed CCTV systems in three U.S. cities, Baltimore, Chicago, and Washington, DC, concluded that the more the system is incorporated into routine law enforcement tactics, the more effectively it may reduce crime.<sup>205</sup> Furthermore, the guidelines published by the police department can address privacy issues as well. A set of rules for routine work could be designed to prevent abuses and to protect the public from the most intrusive aspects of the system.

# **B.** Structural Differences Matter

Similar to China, where public video surveillance cameras are also vastly installed, the United States has relied greatly on the self-restraint of administrative agencies. But due to different political contexts between China and the United States, the relatively uniform, efficient and self-adjusting administrative experience in China may not be fit for the democratic society of the United States. Although the U.S. political system has an affinity with the British political system, the specific traits of U.S. political context has led the practice of regulations to a different path. This part examines two pairs of factors, vertical/horizontal and internal/external, to explain those differences.

http://www.ndrc.gov.cn/zcfb/zcfbtz/201505/t20150513\_691578.html (China).

<sup>&</sup>lt;sup>204</sup> On the influence of such micro-level factors, see Piza E L, Caplan J M, Kennedy L W, *Analyzing the influence of micro-level factors on CCTV camera effect*, 30(2) J. QUANTITATIVE CRIM., 237 (2014).

<sup>&</sup>lt;sup>205</sup> See, La Vigne N, Lowry S, *Evaluation of Camera Use to Prevent Crime in Commuter Parking Lots: a randomized controlled trial.* Urban Institute, Justice Policy Center, Washington, DC, (2011); La Vigne N, Lowry S, Markman J, Dwyer A, *Evaluating the Use of Public Surveillance Cameras for Crime Control and Prevention*, US Department of Justice, Office of Community Oriented Policing Services. Urban Institute, Justice Policy Center, Washington, DC. (2011).

## **Central control analysis (vertical factor)**

The force of the central control may lead to the promulgation of relatively uniform guidelines. In a centralized political system, like China, the central government not only controls resource allocation, but also sets up uniform rules for the whole country. As a result, in the field of public video surveillance, local policies and codes of practice must follow the instructions from the higher authority. In the decentralized political systems like Britain, Australia and the United States, by contrast, local governments are more likely to choose their own guidelines. Thus in the democratic society, the federal government sometimes use the funding method in attempt to induce local governments keep pace with federal priorities.

Federal or central funding for the local deployment of public video surveillance systems is a global practice. In Australia, the \$65.5 million Howard Government funding scheme dubbed "The National Community Crime Prevention Program" (NCCPP) was a major initiative that began in 2004 and ended in 2008 after five rounds of funding. More rounds have since been offered under successive governments.<sup>206</sup> In Britain, government funding took the form of the CCTV Challenge Competition between 1994 and 1999. During this period, £38.5 million was made available for some 585 schemes nationwide. Between 1999 and 2003, major investment was made in public CCTV through the Home Office-funded Crime Reduction Program (CRP). Following a bidding process, a total of £170 million of capital funding was made available to local authorities. As a result of this funding, more than 680 CCTV schemes were installed.<sup>207</sup> The situation in the United States is much more complicated and secretive. But there is no doubt that for the past few years the local governments have received millions of dollars from the federal government through the

<sup>&</sup>lt;sup>206</sup> Carr R., *Surveillance politics and local government: A national survey of federal funding for CCTV in Australia*, SEC. J., 6 (2014) (Austl.)

<sup>&</sup>lt;sup>207</sup> PARKINS, GARRY, ET AL., NATIONAL CCTV STRATEGY, HOME OFFICE, 7 (2007), (U.K.).

Department of Homeland Security grants, even though no exact amount of funding has been disclosed. According to some public available information, "the federal government has spent tens of millions of dollars on Chicago's camera network."<sup>208</sup> Journalists have discovered that "St. Paul, got a \$1.2 million grant for 60 cameras for downtown; Madison, Wis., is buying a 32-camera network with a \$388,000 grant; and Pittsburgh, is adding 83 cameras to its downtown with a \$2.58 million grant."<sup>209</sup> DHS grants even seems to be flowing down to the smallest levels of American law enforcement, bringing Surveillance Cameras to small towns.<sup>210</sup>

The Home Office in Britain has successfully used the funding to influence local practice. A prior study found that the CCTV policy arena has been dominated by central government. Because the impetus for CCTV emanated from central government, the Home Office has endeavored to standardize and centralize technological provision in the local level to meet central government objectives.<sup>211</sup> The CCTV Challenge Competition grants funding to the local government with some requirements such as local matched funding from partnerships and the draft codes of practice. This bidding process is competitive. In the first competition in 1994, the Home Office received bids for 480 schemes, and although the government contribution increased to £5 million, only 106 were funded. In response to the huge demand, there were three further City Challenge Competitions announced between 1995 and 1998. And the central funding took up a big part as up to £31 million in the total £85 million funding of CCTV systems.<sup>212</sup> The central control through a competitive

<sup>&</sup>lt;sup>208</sup> ACLU of Illinois, *supra* note 65.

<sup>&</sup>lt;sup>209</sup> Charlie Savage, US doles out millions for street cameras Local efforts raise privacy alarms, THE BOSTON GLOBE, Aug. 12, 2007,

http://www.boston.com/news/nation/articles/2007/08/12/us\_doles\_out\_millions\_for\_street\_cameras/?page=full. <sup>210</sup> David A. Fahrenthold, *Federal Grants Bring Surveillance Cameras to Small Towns*, WASH. POST, Jan.19, 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/01/18/AR2006011802324.html. <sup>211</sup> Webster, *supra* note 139.

<sup>212</sup> 

Norris, supra note 60, at 112.

bidding process not only encouraged the deployment and stimulated demand beyond that which could be funded,<sup>213</sup> but also spurred the widespread adoption of codes by the police and local authorities because bids without codes of practice draft would fail. Applicants therefore rushed to adopt codes of practice. Without any experience in this field, applicants commonly borrowed from the national model code initiated by the Home Office. Since the vast majority of public CCTV schemes in Britain have entered the Challenge Competition at least once, the vast majority of systems now have similar codes of practice.

In the United States, by contrast, virtually no centralization of surveillance regulations has occurred. First, there are no national statistics about the federal grants on local public video surveillance programs. No single category in DHS grants is designed for the cameras. The spokesman of DHS, Russ Knocke, said that it is difficult to say how much money has been spent on surveillance cameras because many grants awarded to states or cities contained money for cameras and other equipment.<sup>214</sup> Second, there has been a great deal of secrecy regarding the funding process, which makes the research on the central control impossible and any estimation or presumption is vague and unreliable. Matthew Cagle of the ACLU of Northern California explains,

Like the federal intelligence community's black budget, which allows our federal government to allocate billions of taxpayer dollars for spying, all without public debate, these federal grants to local communities also distort the democratic process and prevent a meaningful discussion of the relative costs and benefits of surveillance technology.<sup>215</sup>

<sup>&</sup>lt;sup>213</sup> "For the partnerships of police, local business elites and local authorities the work undertaken to enter a bid created a powerful alliance committed to the installation of CCTV, regardless of the outcome of the competitive process. Many of those who were not successful either found alternative funding strategies or lobbied for another round of competitions." Norris, *supra* note 60, at 122.

<sup>&</sup>lt;sup>214</sup> Savage, *supra* note 209.

<sup>&</sup>lt;sup>215</sup> Sarah Berlin, *Department of Homeland Security funding surveillance on the local level*, BORDC, September 19, 2013, http://www.bordc.org/blog/department-homeland-security-funding-surveillance-local-level.

Third, DHS grants are controversial because they aim to use federal funds to "br[ing] resources and expertise to our law enforcement partners and built new mechanisms to share information,"<sup>216</sup> prompting concerns about converting local police departments and sheriff's offices into "partners" with a massive and lawless federal agency. As a result, some resistance appeared from residents that would be the targets of pervasive public video surveillance. Iowa City imposed a moratorium on some surveillance devices. The Seattle City Council forced its police department to return a federally financed drone to the manufacturer. In Virginia, the state's attorney general said the method of collecting and saving the license plates data collected by cameras violated state law, and the state police purged a database of millions of license plates, including some at political rallies. Even a cash-starved city like Oakland, for which federal financing is very attractive, was forced to add restrictions to its program following a public outcry after the city council approved a surveillance program. The council instructed public officials to write a policy detailing what kind of data could be collected and protected, and how it could be used. The council expects the privacy policy to be ready before the center can start operations.<sup>217</sup>

# Stakeholder analysis (horizontal factor)

Stakeholders involved at the local level may influence the content and process of amending guidelines. Video surveillance programs affect a whole host of government, commercial, organizational, and individual interests, and the shape of administrative regulations depends in large part on which stakeholders wield the greatest amount of influence. As an illustration of stakeholders in U.S. jurisdictions, consider the city of Pittsburgh's CCTV implementation, which

<sup>&</sup>lt;sup>216</sup> DHS website, http://www.dhs.gov/topic/law-enforcement-partnerships.

<sup>&</sup>lt;sup>217</sup> Joe Wolverton, II, J.D. *Federal Grants Enable Increased Surveillance by Local Gov't*, THE NEW AMERICAN, 15 October 2013, http://www.thenewamerican.com/usnews/item/16737-federal-grants-enable-increased-surveillance-by-local-govt.

initially identified 18 different stakeholders that would be affected by the deployment of a sophisticated public surveillance system.<sup>218</sup> More self-identified stakeholders were revealed during the process.<sup>219</sup> Some stakeholders are similar both in the United States and China, including the users of the system, the Mayor, the public safety officials and the vendor. But a large number of stakeholders in China do not have a comparable role in the United States, such as the community groups, the city council and the civil liberties groups.

# (1) Police department

As extremely import stakeholders in both countries, public safety officials in China may play an even more dominant role in the administrative process than their U.S. counterparts. In every corner of the world where public video surveillance is deployed, police departments are undoubtedly the key participants not only in the implementation stage, but also in managing and using the system. In addition, public video surveillance can powerfully influence police officers' behavior.<sup>220</sup> In the implementing stage, police departments find surveillance systems attractive for three reasons highlighted by scholars.

First, the specialization of services in charge of the management of CCTV and / or viewing the resulting images made [police] new professional allies of CCTV development. Then, symbolic rewards that can be derived from the use of CCTV contributed to the enrolment of stakeholders such as municipal police officers, delighted to integrate a "detective" dimension into their daily work, bringing them closer to criminal

<sup>&</sup>lt;sup>218</sup> City of Pgh Housing Authority to use City cameras; Hospitals to rent hospital roof-tops for antennas; Board of Education to use City cameras; Universities to use City cameras; Central Business District to use City cameras for Security & events; Mayor to protect City from crime; City Council to protect City neighborhoods from crime; Constituents/Public to protect City from crime; Community groups/organizations to protect City from crime; Public Safety Officials (police/fire/EMS) to assist public safety officials perform job; District Attorney to serve as an investigative tool; Coast Guard to protect waterways and rivers; Media to collect/disseminate info. to the public; City's Chief Information Officer to design infrastructure/manage project; Technologists to design infrastructure; Vendors to sell product; Civil liberty groups to protect civil liberties; City lawyers to prepare contract & ensure compliance. Citing table 1, Mu, Enrique and Stern, Howard A., *A Structured Stakeholder Self-Identification Approach for the Deployment of Public Information Systems: The Case of Surveillance Technology in the City of Pittsburgh*, 23 J. INFORM. TECH. MGMT, 50 (2012).

<sup>&</sup>lt;sup>220</sup> Goold B J, *Public area surveillance and police work: the impact of CCTV on police behavior and autonomy*. 1(2) J. SURVEILLANCE & SOCSU, 191 (2003).

investigation, which would normally be the responsibility of the National, not Municipal, Police. Lastly, the National Police force appreciated the 'cost-free' resource of CCTV, using a device they do not have to finance but according their own professional priorities: law enforcement or criminal investigation in particular.<sup>221</sup>

Police departments are also the main user of video surveillance systems. In 2014 at the China Smart City Innovation Conference, the chief engineer of the Technology and Information Bureau of the Ministry of Public Security, Zhu Fugang, revealed based on incomplete statistics that China's public security organs have used video surveillance service nearly 42 million times, and served the people nearly 10 million times in 2013.<sup>222</sup>

Administrative guidelines' functional provisions, such as limiting public video surveillance, creating operational procedures and regulating police officers' behavior, are mostly published by the police department itself. But the degree of freedom police departments enjoy in crafting those regulations depends on their institutional strength. A relatively weak, politically dependent police department may be accountable to a wide range of stakeholders as it designs guidelines.. By contrast, a powerful and independent police department, subject to little external influence, only needs to follow its own internal rules, which are presumed to meet the department's interest to the utmost extent.

The institutional strength of police departments is another point of distinction between Chinese political practice and that of the United States. "China has a one-party political system, a tradition of centralized government, and a highly politicized and centralized police structure,"<sup>223</sup>

<sup>222</sup> Gong 2 Bu Jiang Jiada Shipin Jiankong Xitong Fugai Huo Quan Hangye Dailai Lihao.(公安部将加大视频监控 系统覆盖或全行业带来利好)[The Ministry of Public Security will enhance the coverage of CCTV, may benefit the whole industry], Zhengquan Shibao Wang (证券时报网), Nov. 7, 2014,

http://kuaixun.stcn.com/2014/1107/11835126.shtml. (China).

<sup>&</sup>lt;sup>221</sup> Germain S, Dumoulin L, Douillet A C. *A prosperous 'business'*. *The success of CCTV through the eyes of international literature*. 11(1/2) SURVEILLANCE & SOCVE, 134,143 (2013).

<sup>&</sup>lt;sup>223</sup> Cao L, Hou C, *A comparison of confidence in the police in China and in the United States*, 29(2) J. CRIM. JUS., 87 (2001).

however, "the U.S. has a predominantly two-party political system, a tradition of federal government, and a multilevel and often fragmented police structure."<sup>224</sup>

In China, the police department is a special department in the government. The renowned Chinese scholar, Professor Chen Xingliang explains that in China the police department holds vast and important power, not only undertaking the criminal justice function, but also performing a variety of administrative management functions, including security, road traffic management, fire supervision, Census Management and so on. Its authority is powerful and can influence every facet of the society.<sup>225</sup> One sign of that power is the position of the police chief in the local government structure. At the provincial, municipal, and county levels, the police chief also simultaneously serves the deputy of the government at the same time. Thus, the police department plays dominant role in the decision-making process, especially in the fields relevant to the public safety and social control. Barely none could question its authority. When local police departments follow the instruction from their higher authority to deploy and use public video surveillance, they often get absolute support from the local government and encounter few obstacles as long as the funding can be arranged. After the demand of the police department was accepted by the local government, a committee would be set up to coordinate various relevant departments, which would simply obey the unified plan for the project. Thus, the government-owned camera systems in China are essentially a product of police self-construction.<sup>226</sup>

On the other hand, the U.S. police departments must compromise far more often in light of

<sup>&</sup>lt;sup>224</sup> Id.

<sup>&</sup>lt;sup>225</sup> Ye Zusheng(叶竹盛), Gongong Juzhang de Quanli Chang (公安局长的权力场)[The power games of the Police Chief], 5 Renmin Wenzhai (人民文摘,第5期) (2012). http://paper.people.com.cn/rmwz/html/2012-05/01/content 1059394.htm (China).

<sup>&</sup>lt;sup>226</sup> Yang Jianguo (杨建国), Lun Shipin Jiankong de Fanzui Yufang Gongneng ji Fanzui zhengcha Jiazhi (论视频监 控的犯罪预防功能及犯罪侦查价值)[CCTV's Crime Prevention Functions and Crime Investigation Values], Fanzui Yanjiu (犯罪研究), 66, 2011 年第 1 期 (China).

the many stakeholders involved, including a multitude of neighborhood groups, community organizations, and businesses that maintain or might desire to install independent surveillance systems. In Pittsburgh's case study, the surveillance system committee, comprised of different groups that represented many varying interests, believed that all possible stakeholders had been considered. But one unexpected stakeholder appeared, the Fraternal Order of Police (police union) even demanded a voice in the deployment plan just because they were afraid of the potential for the City to use surveillance to continuously scrutinize the police force and constantly conduct video review of the police officer's conduct in the field.<sup>227</sup>

## (2) The vendor

The fact that vendors of video surveillance products can influence the decision to install systems was revealed in early studies in Britain, which showed that "the open-street CCTV was the result of a strategic alliance between local government and local economic interests."<sup>228</sup> Similarly, in China, a study stated that public video surveillance has become a money-earning tool for some enterprises and local governments.<sup>229</sup> But spurring the implementation of a system is one thing; influencing the regulations is another. Currently, both in China and the United States, the CCTV industry's direct or indirect impact on the regulations adopted by the executive branches has not been fully studied. Nonetheless, it is safe to estimate that this factor may play a modest role in administrative regulations in both countries. After successfully lobbying government to install the system, the only work left for the vendor is to meet the specific demands of the

<sup>&</sup>lt;sup>227</sup> Mu, Enrique and Stern, Howard A., *A Structured Stakeholder Self-Identification Approach for the Deployment of Public Information Systems: The Case of Surveillance Technology in the City of Pittsburgh*, 23 J. INFORM. TECH. MGMT, 57 (2012).

<sup>&</sup>lt;sup>228</sup> Germain, *supra* note 221..

<sup>&</sup>lt;sup>229</sup> Liu Chengbo(刘成波), Gonggong Changsuo Shipin Jiankong de Falv Guizhi—uizYinsiquan Baohu wei Shijjiao(公共场所视频监控的法律规制——以隐私权保护为视角) [The Legal Regulations of Video Surveillance in Public Places: From the Perspective of Privacy Protection.] 18 (2013) (M.S. thesis, Jilin University.) (China).

government based on the available technologies in the regulating context. Thus, vendors have fewer motives to influence the operational and administrative practice in the post-deployment stage than to influence the legislation. But we have to acknowledge that commercial interests may still have some influence on executive self-regulation, even though the evidence is limited.

# (3) City Council and civil liberties groups

With the dominant police department and the supportive local government behind, there is little room left to other stakeholders in China. In particular, there is no room for the City Council or civil liberties groups, both of which play a significant part in the formation of privacy policy in the United States. Before the decision to start the project in the U.S., the privacy policy would be presented to City Council for approval. Developing a draft policy in Pittsburgh took approximately nine months, and during that period the City held public fact-finding meetings with all identified stakeholders, including industry experts and representatives from various community and civil liberties groups, to discuss the nuances and feasibility of the proposed policy.<sup>230</sup> The development of codes of conduct in Britain follows a similar pattern. The ongoing work of civil liberties groups appears to have had a considerable impact on the thinking and priorities of the police and local authorities regarding the use of CCTV and the need for regulation.<sup>231</sup> It has been also instrumental in drawing the attention of the public to the need for greater control and regulation of this technology.<sup>232</sup>

# Effectiveness analysis (internal factor)

As discussed in Part I, the research by scholars has raised considerable concern about the

<sup>&</sup>lt;sup>230</sup> Mu, *supra* note 227, at 60.

<sup>231</sup> 

GOOLD, supra note 199, at 102.  $^{232}$  *Id*.

effectiveness of video surveillance. That research could help to inform the objectives the system aims to achieve. The findings that the CCTV is more effective in one setting than others may also help answer questions like, how many cameras are needed and where? Research on the costs of surveillance systems may prompt the consideration of other possible alternatives.

No government can avoid addressing considerations of effectiveness, which play a big role in justifying monitoring, but there are important differences in the way that policymakers in China and the United States evaluate effectiveness. The first difference concerns the content of the effectiveness considerations. Governments in the United States focus mainly on effectiveness in combatting crime and terrorism, as reflected in the NYPD guidelines and in the sources of funding for these programs. Two scholars, Rajiv Shah and Jeremy Braithwaite, have identified two dominant justifications for cameras have emerged in the United States. One is for police investigations where cameras are used to solve crimes after they occurred. The other for cameras is reducing or preventing crime.<sup>233</sup> In China, by contrast, the implementation of the Golden Shield Project places more emphasis on the sociological processes to create a national surveillance.

Walton reports that the project was launched:

to promote "the adoption of advanced information and communication technology to strengthen central police control, responsiveness, and crime combating capacity, so as to improve the efficiency and effectiveness of police work." China's security apparatus announced an ambitious plan: to build a nationwide digital surveillance network, linking national, regional and local security agencies with a panoptic web of surveillance. Beijing envisions the Golden Shield as a database-driven remote surveillance system – offering immediate access to records on every citizen in China, while linking to vast networks of cameras designed to increase police efficiency.<sup>234</sup>

Interestingly, a second difference in how U.S. and Chinese officials evaluate effectiveness

<sup>&</sup>lt;sup>233</sup> Shah R, Braithwaite J, *Spread too thin: Analyzing the effectiveness of the Chicago camera network on crime*, 14(5) POLICE PRAC. & RES., 415 (2013).

<sup>&</sup>lt;sup>234</sup> WALTON, G. (2001), CHINA'S GOLDEN SHIELD: CORPORATIONS AND THE DEVELOPMENT OF SURVEILLANCE TECHNOLOGY IN THE PEOPLE'S REPUBLIC OF CHINA, (2001).

lies in the timing of when governments consider it. The United States prefers *ex ante* analysis while the China likes *ex post* analysis, and that difference has shaped the development of surveillance systems in the two countries.

The U.S. executive branch generally prefers to conduct cost-benefit analysis before engaging in a new project. Local public video surveillance advocates therefore need to persuade the City Council, the public and various partnerships and stakeholders that there is imminent necessity to set up public video surveillance in the name of public safety. For example,

The city of Chicago claims cameras have reduced crime. Specifically, cameras reduced serious index crimes by 17% in the monitored areas. Overall, the police claimed a drop of 30% in crime in the 234 areas where cameras were located. The cameras were also touted as a significant factor in reducing homicides 25% between 2003 and 2004. As a result, the Chicago experience has provided the imprimatur of effectiveness for large-scale camera networks. Other cities such as Baltimore and New York use the Chicago experience to justify additional cameras.<sup>235</sup>

However, in the starting stage, Chinese police departments generally do not consider the effectiveness of the system as much as their U.S. counterparts. The benefits of surveillance programs cited by proponents are in general terms, and often lack supportive evidence. But that would not be an obstacle in China, where effectiveness evaluation does not occur until after implementation. And even then, the process may be distorted due to "the objective management and the performance assessment," which pervades the administrative departments throughout the whole country. "The objective management and the performance assessment" is conducted by the superior departments to evaluate their subordinate organs based on several indexes set up by themselves. The installing, operating and using of public video surveillance were some of the indexes that formed part of the assessment. As a result, the deployment of public video surveillance started before any meaningful and systematic evaluation of its effectiveness.

<sup>&</sup>lt;sup>235</sup> Braithwaite, *supra* note 233.

In China, one key index to evaluate whether the system has functioned properly lies in a mechanism called "Typical Case Reporting System." A monthly quota is set up by the high authority, asking the operators to report typical cases in which the public video surveillance system plays a part—for example, to help investigate criminal cases, to help keep social order, to monitor traffic violations or to provide any other valuable information. Operators have to collect the complete information about the events relevant to the use of cameras, and submit them to the higher authority along with video or pictures distilled from the surveillance system. These typical cases are then selected and used by the higher authority to meet department objectives or to publicize what the police have done to reduce crimes and protect people.<sup>236</sup> The typical case reporting system is the primary mechanism by which departments take the effectiveness into consideration. If a local police department has met the quota of "typical cases," public video surveillance there will be taken as an effective tool for the police to use.

Objectively speaking, this *ex post* administrative evaluation of the performance of the operators and users does somehow spur the operational work and encourage the use of this system, which will help the system accomplish effectiveness in a long run. According to publicly available reports, the police departments in Shanxi Province had successfully used the public video surveillance in 13,321 cases in 2014, including 1,655 criminal cases. Meanwhile, the total number of the cameras in the public places has increased to 148,631 feeds in the whole province.<sup>237</sup> Within

<sup>&</sup>lt;sup>236</sup> Zhang Lianhan (张潋瀚), An Empirical Study on the Operational Mechanism of Skynet Surveillance (天网监控 运行机制实证研究), (2014) (unpublished M.A. Thesis, Sichuan University) (China).

<sup>&</sup>lt;sup>237</sup> Chang Jian, Zhang Chengming (常健、张成明), Shanxi Gongan Jiguan Yinian Jiezhu Jiankong Shipin Poopi 13321 Qi. (山西公安机关一年借助监控视频破案 13321 起) [The Police in Shanxi Province has solved 13321 cases by using CCTV], Huanghe Xinwen Wang (黄河新闻网), Feb. 9, 2015, http://law.sxgov.cn/content/2015-02/09/content\_5550768.htm. (China).

the Huanpu district of Guangzhou, where 16,000 feeds have been installed, there were 703 criminal cases with the video surveillance assistance in 2014. The number of cases directly or indirectly using the cameras take up 57.7% in the total number of detected cases.<sup>238</sup> But in practice, these fancy numbers which are used to prove the effectiveness one of systems in particular precincts should be discounted. Operators trying to meet their quota, a task which could eventually influence their performance evaluation and income, could retrospectively apply the cameras. For example, one empirical study recounted a case in which an operator used video data in the system to illustrate that how a crime was detected. But in fact, the operator had followed the clues to find the video out after the police had detected that crime by other measures.<sup>239</sup>

### The public attitude analysis (external factor)

A final factor to consider is public opinion, as distinguished from the views of specific individual stakeholders. Political science defines public opinion as "the aggregate of public attitudes or beliefs about government or politics."<sup>240</sup> Those dynamic attitudes have the power to influence the government. Civil liberties groups who are stakeholders may be taken as the representatives of the public, but they cannot replace the public, for whom the government acts and whose views should be respected.

Analyses of public opinion on public video surveillance have produced mixed results, and

<sup>&</sup>lt;sup>238</sup> Huangpu Gonggpu Fenju (黄埔公安分局), 1.6 Wan Ge Shipin Jiankong Dian Quan Fugai, Qunian Huangpu Jinfang Kantu Pootu 703 Zong.(1.6 万个视频监控点全覆盖,去年黄埔警方看图破案 703 宗)[16000 cameras cover, the police of Huangpu has solved 703 cases last year], Fenghuang Wang (凤凰网), Jan. 19, 2015, http://gz.ifeng.com/zaobanche/detail\_2015\_01/19/3449235\_0.shtml (China).

<sup>&</sup>lt;sup>239</sup> Zhang Lianhan, *supra* note 244.

<sup>&</sup>lt;sup>240</sup> BIANCO, WILLIAM T., AND DAVID T. CANON, *Public Opinion*, In AMERICAN POLITICS TODAY (3rd ed. New York: W.W. Norton, 2013).

may be hampered by methodologically questionable social surveys.<sup>241</sup> However, studies that have measured levels of support for CCTV have shown a clear and strong public support among most countries.

Studies in Britain in 1992 and in 2005 found that public support for CCTV remains high.<sup>242</sup> The report in 2005 presented the people's attitude to CCTV in 12 areas. It showed 82% of the respondents, who had no prior knowledge and experience of CCTV in their area, were happy with CCTV being installed. The finding in town and city centers also mirrored that for residential areas. At the same time, the public remained unaware of the capabilities of CCTV, even as they expected it was having an impact on crime in their residential area. <sup>243</sup>

A comparative survey from Canada and the USA found that people far more confident about the effectiveness of camera surveillance than are researchers on the topic. For example, in 2006 and 2012, the U.S. remained at a steady 71% in the belief in effectiveness for community CCTV.<sup>244</sup> Researchers found that result discouraging: "they are more knowledgeable about the technologies and that they have a say over their data-travels but fewer actually know about laws governing personal data and, for those who use them, their preferred modes of self-protection vary considerably."<sup>245</sup>

In China, there is no published research providing any number about the public attitude

<sup>242</sup> See Honess, T. and Charman, E., *Closed circuit television in public places: its acceptability and perceived effectiveness.* POLICE RESEARCH GROUP CRIME PREVENTION UNIT, 35 (1992) (U.K.). ARGOMANIZ J, GILL M, BRYAN J, PUBLIC ATTITUDES TOWARDS CCTV: RESULTS FROM THE PRE-INTERVENTION PUBLIC ATTITUDE SURVEY CARRIED OUT IN AREAS IMPLEMENTING CCTV, (Home Office, 2005).

<sup>&</sup>lt;sup>241</sup> Jason Ditton showed that public support for CCTV varied by a margin of 35 points according to the questionnaire design. Ditton, J. *Crime and the City: Public attitudes towards open-street CCTV in Glasgow.* 40 (4) BRITISH JOURNAL OF CRIMINOLOGY, 692 (2000) (U.K.).

<sup>&</sup>lt;sup>243</sup> ARGOMANIZ J, GILL M, BRYAN J, PUBLIC ATTITUDES TOWARDS CCTV: RESULTS FROM THE PRE-INTERVENTION

PUBLIC ATTITUDE SURVEY CARRIED OUT IN AREAS IMPLEMENTING CCTV, 48 (Home Office, 2005). <sup>244</sup> Smith, E. A. and Lyon, D, *Comparison of Survey Findings from Canada and the USA on Surveillance and Privacy from 2006 and 2012*. 11(1/2) SURVEILLANCE & SOC'Y 190,196 (2013). http://www.surveillance-and-society.org

 $<sup>^{245}</sup>$  Id, at 202.

towards the public video surveillance. Just according to a field research in which the author of this paper took part in 2012, the survey showed that 93.7% (including very supportive and fairly supportive) of 478 people in two middle-class counties supported the public surveillance system.<sup>246</sup>

Why do people support a project that they do not fully understand? This question raised some scholars' interest, and some of their findings point to the media's role in shaping public acceptance of cameras. Mass media, after all, benefit from video surveillance systems. The images captured by surveillance cameras can make the news seem more authentic and vivid. Thus, the media becomes one part of the loop that encourages the expansion of video surveillance systems. As the gatekeepers of the system who can get access to the images, the police department could choose to provide information to the media when doing so is in the department's interest. Images of crime shown on television news programming could increase the public anxiety of the risk of crimes. Anxiety, in turn, spurs more calls for further extension of public video surveillance systems that lead to more crime events being captured on video and played on the media.<sup>247</sup> For the news media covering the system, the cameras are seen as friendly eyes, leaving the effectiveness and legitimacy

of the system unquestioned:

Since the early 1990s, CCTV has spread out visibly into the public realm, and cameras are now connected to public efforts to combat crime, which means they have achieved a public value that is immediately reflected in the media. Yet, especially in the UK, any critical debate seemed to be banned from the beginning.<sup>248</sup>

In other words, before CCTV became a reality of everyday life it first of all became a part of news stories and nationwide television shows.<sup>249</sup>

<sup>&</sup>lt;sup>246</sup> Unpublished materials. Ma Jinghua, Zhang Lianhan (马静华, 张潋瀚), SiChuan Shuangliu and Hongya public opinion surveys. (四川省双流县、洪雅县公众意见问卷调查分析) (on file with author) (China).

<sup>&</sup>lt;sup>247</sup> Surette, *supra* note 21.

<sup>&</sup>lt;sup>248</sup> Hempel L, Tempel E, *The Surveillance Consensus Reviewing the Politics of CCTV in Three European Countries*, 6(2) EUROPEAN J. CRIM., 157, 166 (2009).

<sup>&</sup>lt;sup>249</sup> Id, at 167.

In addition, Rachel L. Finn and Michael McCahill have argued that media portrayals of surveillance "continue to reinforce existing social divisions by marking out clear distinctions between 'us' (law abiding citizens) and 'them' ('deviants' and 'outgroups')."<sup>250</sup> The public is depicted as a group of law abiding citizens who will "put up with" increasing levels of surveillance in order to get security and safety. To dissent in terms of increasing the amount of CCTV cameras would put people on the side of "them."<sup>251</sup>

Aside from the media, there are several other possible explanations for high levels of public support. A leading surveillance expert, Professor David Lyon, argues that individuals rarely feel oppressed by the surveillance by the powers, noting that a majority will even actively collaborate by giving personal data, considering the benefits to be higher than the cost.<sup>252</sup> Professor Didier Bigo proposed a notion, the "ban-opticon," <sup>253</sup> which indicates only the few profiled as "unwelcome" are monitored by a few, to alternate the "panopticon"<sup>254</sup> and "synopticon."<sup>255</sup> The ban-opticon stresses exceptional cases, including the exclusion of certain groups, the exceptionalism of power and the production of normative imperatives within post 9/11 discussions. What makes the ban-opticon especially interesting is that "the visibility of exclusion vanishes, while the power of exception and the production of normative imperatives amalgamate into a "governmentality" of uncertainty, unease, fear and (in)security."<sup>256</sup> Meanwhile, Professor Gary T.

<sup>&</sup>lt;sup>250</sup> Finn, R. and M. McCahill. *Representing the Surveilled: Media Representations and Political Discourse in Three UK Newspapers*, POL. STUD. ASS'N CONF. PROC., 2 (2010).

<sup>&</sup>lt;sup>251</sup> Kroener, *supra* note 22.

 <sup>&</sup>lt;sup>252</sup> LYON, D. SURVEILLANCE SOCIETY. MONITORING EVERYDAY LIFE, (Buckingham: Open University Press 2005).
<sup>253</sup> BIGO, D. Security, Exception, Ban and Surveillance. In THEORIZING SURVEILLANCE: THE PANOPTICON AND BEYOND, 46 (D. Lyon ed., Uffculme: Willan. 2006).

<sup>&</sup>lt;sup>254</sup> The theory of surveillance in terms of Foucault's notion of the panopticon, a few control the many, thereby emphasising self-discipline.

<sup>&</sup>lt;sup>255</sup> Mathiesen's notion the 'viewer's society, where many watch the few by media coverage in the press, on television and the Internet.

<sup>&</sup>lt;sup>256</sup> Hempel, *supra* note 248, at 161.

Marx has characterized new surveillance as having a tendency to become abstract. This abstract character of new surveillance almost invalidates opposition.<sup>257</sup> Both the exception and the abstract character of surveillance result in an expectation that nobody (including the judges) asks for the legitimacy and the efficiency after a certain period of time.

The high-level public support and low-level doubt on the legitimacy and efficiency of public video surveillance do not mean the governments can do whatever they want, especially in a democratic society where the people's political beliefs value freedom.

In China, the government may obtain the political trust through other measures, like cultural factors. Chinese scholar Ma Deyong explains that "[i]n a country with a history of autocratic or authoritarian rule, people's trust in government is not only based on the government's performance, but also on people's worship of authority and dependence."<sup>258</sup> Thus, the people may take the government's specific decisions on public video surveillance issues for granted as long as they have been told that all of those are to protect them. Furthermore, according to a study, Chinese people are less concerned about privacy right for three main reasons: the long tradition of collectivism that trumps individualism, the tight control by the government and close scrutiny of citizens, and the average crowded living environment where private space is not generally expected.<sup>259</sup>

Those cultural factors do not have the same force in the United States. Instead, rational choice theory is a starting point of the theoretical analysis of the causes of political trust in western

<sup>&</sup>lt;sup>257</sup> Marx, G. T., *What's New About the 'New Surveillance'? Classifying for Change and Continuity*, SURVEILLANCE AND SOCVE, 9 (2002).

<sup>&</sup>lt;sup>258</sup> Ma Deyong (马得勇), Zhengzhi Xinren Jiqi Qiyuan—iyuaYazhou 8 Ge Guojia he Diqu de Bijiao Yanjiu (政治信 任及其起源——对亚洲 8 个国家和地区的比较研究) [Institutional and Cultural Factors of Political Trust inEight Asian Societies]. 5 Jingji Shehui Tizhi Bijiao (经济社会体制比较), 79 (2007) (China).

<sup>&</sup>lt;sup>259</sup> R. Tang. 2002. Approaches to Privacy – The Hong Kong Experience. (citing from Yao-Huai L. Privacy and data privacy issues in contemporary China, 7(1) ETHICS AND INFORMATION TECHNOLOGY, 7, 12 (2005) (China).

countries. The people can be presumed as reasonable individuals with rational judgments.<sup>260</sup> Citizens care about their freedom and privacy right with a relatively longer history of privacy protection, so there can be always concerns about encroachment on civil liberties. Besides, the public participation is always one of key elements in the democracy. All of these result in a necessity for the democratic government to involve public participation in the decision-making process as fully as possible.

# V. Conclusion

As a democratic and free country, the United States might have gone on a different path regarding regulating public video surveillance, either from Britain with its similar political system or from China with a totally different one. The three branches of government in the U.S. are deadlocked and unable to take any meaningful actions. The Supreme Court, which is in a strong position to set national and uniform standards for privacy protection, has not found a way to break away from its own precedents. The legislative branch can do little on the national level regulations due to federalism and the distribution of law enforcement activities at the state and local level. Local legislative efforts might be helpful, but the process in each place will be complicated by concerns about public security, the interests of industry, and politicians' imperative to take visible actions like video surveillance to fight against crimes and protect people, especially in the post-9/11 context. The executive branch might be the weakest point in the deadlock because it already bears responsibility for resolving tensions between privacy and safety. As the main advocates for and daily users of the system, police departments must make rules for the purpose of manage

<sup>&</sup>lt;sup>260</sup> Ma Deyong, *supra* note 258.

complex surveillance systems and to avoid arbitrariness.

In the absence of action by the judicial and the legislative branches, self-restraint by the executive branch has become crucial in determining the actual privacy protection the people can obtain under pervasive video surveillance. Without the ordinary forms of judicial and legislative oversight, the possibility of abuse by the executive branch may increase. Also, unlike China, the United States' local governments are not accountable to a single national authority. They must be accountable to the people. As a result, the public participation in the United States is more necessary in the decision-making process regarding public video surveillance.

Public opinion remains supportive of public video surveillance systems due to complicated and intertwined factors. People are worried about the safety and security, and the mass media exaggerates the effectiveness of the system in preventing crimes or terrorism. The public are not well informed privacy issues brought by video surveillance. The executive branch uses the risk that criminals might take advantage of surveillance information as an excuse, refusing to disclose even basic information about the system, such as the funding sources, the total number and location of cameras, etc., not to mention any incidents that have invaded people's rights. But ample research has demonstrated that the crime-prevention effectiveness of public surveillance is doubtful. And the practice in China that the police department initially publish the typical cases can help relieve the concern that this kind of information could be illegally used by the criminals.

These doubts about effectiveness do not inevitably lead to a conclusion that public video surveillance is useless and should be abandoned. There have been a lot of studies showing that public video surveillance is not only about the ability to prevent and detect crime, just like Clive Norris stated: "It is about the power to watch, to deploy, to intervene, to identify and to regulate, often through exclusion...it concerns the reproduction of order."<sup>261</sup> The new functions need new justifications to balance the privacy danger, at the same time, the adequate regulations are also needed to keep the threats to privacy at the minimum.

Back to 2008, the Home Affairs Committee in Britain rejected "crude characterizations of our society as a surveillance society." It drew a line to define the surveillance society. As long as trust in the government's intentions in relation to data and data sharing is preserved, the society could not be described as a surveillance society even there are trends of automatization, function creep and integration of surveillance systems.<sup>262</sup> Indeed, this statement could be seen as a call for visibility and vocalization. If the government wants to meet its accountability promise to the public, it has to initially disclose the information about the system and to involve more public participation in the deployment, management and usage stages. After all, the public support is the key in the democratic society.

# **Bibliography**

### Cases

N.Y. Civil Liberties Union v. Dep't of Homeland Sec., 771 F. Supp. 2d 289 (S.D.N.Y. 2011).

California v. Ciraolo, 476 U.S. 207, 215 (1986).

United States v. Jones, 132 S. Ct. 945 (2012).

Handschu v. Special Services Div., 605 F.Supp. 1384, 1421 (S.D.N.Y. 1985), aff 'd, 787 F.2d 828 (2d Cir. 1986).

Handschu v. Special Services Div, 288 F.Supp.2d 411, 422 (S.D.N.Y. 2003)

Katz v. United States, 389 U.S. 347 (1967).

 <sup>&</sup>lt;sup>261</sup> NORRIS, C., *The success of failure: Accounting for the Global Growth of CCTV*. In: ROUTLEDGE INTERNATIONAL HANDBOOK OF SURVEILLANCE STUDIES, 258 (eds K.S. Ball, K.D. Haggerty and D. Lyon. London: Routledge, 2012).
<sup>262</sup> Hempel, *supra* note 248, at 174.

United States v. Knotts, 460 U.S. 276, 282 (1983).

California v. Ciraolo, 476 U.S. 207, 207, 106 S. Ct. 1809, 1810, 90 L. Ed. 2d 210 (1986).

Kyllo v. United States, 533 U.S. 27. (2001).

New York Civil Liberties Union v. Dep't of Homeland Sec., 771 F. Supp. 2d 289, 290 (S.D.N.Y. 2011)

United States v. Taborda, 635 F.2d 131(2d Cir. 1980).

State v. Thomas, 642 N.E.2d 240, 246(Ind. Ct. App. 1994).

State v. Bonnell, 856 P.2d 1265, 1277(Haw. 1993).

State v. Costin, 720 A.2d 866 (Vt. 1998).

Cowles v. State, 23 P.3d 1168, 1171 (Alaska 2001).

United States v. Alfonso D. Lopez, Jr., 514 U.S. 549.

United States v. Garcia, 474 F.3d 994, (7th Cir. 2007).

Buckley v. Am. Constitutional Law Found, 525 U.S. 182 (1992).

NAACP v. Alabama ex rel. Patterson, 357 U.S. 449 (1958).

#### <u>Statutes</u>

U.S. Patent 3114797, 1963.

U.S. Patent 3590151, 1966.

5 U.S.C.A. § 552(b) (7).

5 U.S.C. § 552a (1994).

5 U.S.C. § 552a (o) (1994).

42 U.S.C. § 2000(aa)-(aa) (12) (1994).

12 U.S.C. §§ 3401-3422 (1994).

#### Periodical Materials

Aileen B. Xenakis, Washington and CCTV: It's 2010, not 1984, 42 CASE W. RES. J. INT'L L. 573

(2010).

Olivia J. Greer, *No Cause of Action: Video Surveillance in New York City*, 18 MICH. TELECOMM. & TECH. L. REV. 589 (2012).

Adam Schwartz, *Chicago's Video Surveillance Cameras: A Pervasive and Poorly Regulated Threat to Our Privacy*, 11 Nw. J. TECH. & INTELL. PROP. 47 (2013).

Hilton Collins, *Video Camera Networks Link Real-time Partners in Crime Solving*, GOVT. TECH. (Feb, 1, 2012)

Jerry Kang, Information Privacy in Cyberspace Transactions, 50 STAN. L. REV. 1193 (1998).

Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 MINN. L. REV. 407 (2012).

Kevin Miller, *Total Surveillance, Big Data, and Predictive Crime Technology: Privacy's Perfect Storm*, 19 J. TECH. L. & POL'Y 105 (2014).

Robb, Gary C., *Police Use of CCTV Surveillance: Constitutional Implications and Proposed Regulations*, U. MICH. J. L. REFORM, 572 (1979).

Surette R., The thinking eye: *Pros and cons of second generation CCTV surveillance systems*. 28(1), POLICING: INT'L J. POLICE STRATEGIES & MGMT., 152 (2005)

Kroener I., "Caught on Camera": The media representation of video surveillance in relation to the 2005 London Underground bombings. 11(1/2) SURVEILLANCE & SOC'Y, 121 (2013). (U.K.).

Porikli F, Brémond F, Dockstader S L, et al. *Video surveillance: past, present, and now the future*. 30(3) IEEE SIGNAL PROCESSING MAGAZINE, 190 (2013).

Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 Minn. L. Rev. 407 (2012).

Klontz J C, Jain A K, *A case study on unconstrained facial recognition using the boston marathon bombings suspects*, 13 Michigan State University Technical Report MSUCSE, 4 (2013).

Wechsler, Harry, et al., eds. *Face recognition: From theory to applications*, 163 SPRINGER SCIENCE & BUSINESS MEDIA, (2012).

Pagano C, Granger E, Sabourin R, et al. *Adaptive ensembles for face recognition in changing video surveillance environments*, 286 INFORMATION SCIENCES, 75 (2014).

Bhaltilak K V, Kaur H, Khosla C., *Human Motion Analysis with the Help of Video Surveillance: A Review*, 4(9) INT'L J. COMPUTER SCI. ENGINEERING TECH (IJCSET), 245 (2014).

Margaret Hu, Biometric Id Cybersurveillance, 88 Ind. L.J. 1475 (2013).

Campbell, D. and Ross, L., *The Connecticut crackdown on speeding*, 3 LAW & SOC'Y REV., 33 (1968).

Clarke, M., Blind eye on the street? POLICE REV., August, 29 (1994).

Ratcliffe, J., Taniguchi, T., & Taylor, R. B, *The crime reduction effects of public CCTV cameras:* A multi-method spatial approach. 26 JUSTICE QUARTERLY, 746 (2009).

McLean S J, Worden R E, Kim M S., *Here's Looking at You An Evaluation of Public CCTV Cameras and Their Effects on Crime and Disorder*, 38(3) CRIM. JUSTICE REV., 303 (2013).

Stutzer A, Zehnder M. *Is camera surveillance an effective measure of counterterrorism*? 24(1) DEF. & PEACE ECON., (2013).

Olivia J. Greer, *No Cause of Action: Video Surveillance in New York City*, 18 MICH. TELECOMM. & TECH. L. REV. 589 (2012).

Newell, Bryce Clayton, Local Law Enforcement Jumps on the Big Data Bandwagon: Automated License Plate Recognition Systems, Information Privacy, and Access to Government Information (October 16, 2013). 66 ME. L. REV., 398 (2014).

Robert R. Belair & Charles D. Bock, *Police Use of Remote Camera Systems for Surveillance of Public Streets*, 4 COLUM. HUM. RTS. L. REV. 143 (1972).

Stephen E. Henderson, Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search, 56 Mercer L. Rev. 507 (2005).

Stephen Rushin, *The Judicial Response to Mass Police Surveillance*, U. ILL. J.L. TECH. & POL'Y, 281 (2011).

Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213 (2002).

G. Wade, Funding CCTV: The Story So Far, 7 CCTV TODAY 28 (1998).

Jeremy Brown, *Pan, Tilt, Zoom: Regulating the Use of Video Surveillance of Public Places*, 23 BERKELEY TECH. L.J. 755 (2008).

Webster CWR, *CCTV policy in the UK: Reconsidering the evidence base*, 6 (1) SURVEILLANCE & SOC'Y, 10 (2009).

Stuart Minor Benjamin, *Stepping into the Same River Twice: Rapidly Changing Facts and the Appellate Process*, 78 TEX. L. REV. 269 (1999).

Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801 (2003-2004).

Joyce W. Luk, *Identifying Terrorists: Privacy Rights in the United States and United Kingdom*, 25 HASTINGS INT'L & COMP. L. REV. 223 (2002).

Michael W. Heydrich, *A Brave New World: Complying With the European Union Directive on Personal Privacy Through the Power of Contract*, 25 BROOK. J. INT'L L. 407 (1999).

Peter Mei, The EC Proposed Data Protection Law, 25 LAW & POL'Y INT'L BUS. 305 (1993).

Joyce W. Luk, *Identifying Terrorists: Privacy Rights in the United States and United Kingdom*, 25 HASTINGS INT'L & COMP. L. REV. 223 (2002).

Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1 (2008-2009).

Orin S. Kerr, *The National Surveillance State: A Response to Balkin*, 93 MINN. L. REV.2179 (2009).

Daniel J. Solove, *Digital Dossier and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083 (2002).

Westin, A. F., Social and Political Dimensions of Privacy, 59 J. Soc. ISSUES, 431 (2003).

David Lyon, *Globalizing Surveillance Comparative and Sociological Perspectives*, 19(2) INT'L SOC., 135 (2004).

Piza E L, Caplan J M, Kennedy L W, *Analyzing the influence of micro-level factors on CCTV camera effect*, 30(2) J. QUANTITATIVE CRIM., 237 (2014).

La Vigne N, Lowry S, *Evaluation of Camera Use to Prevent Crime in Commuter Parking Lots: a randomized controlled trial.* Urban Institute, Justice Policy Center, Washington, DC, (2011).

La Vigne N, Lowry S, Markman J, Dwyer A, *Evaluating the Use of Public Surveillance Cameras for Crime Control and Prevention*, US Department of Justice, Office of Community Oriented Policing Services. Urban Institute, Justice Policy Center, Washington, DC. (2011).

Carr R., *Surveillance politics and local government: A national survey of federal funding for CCTV in Australia*, SEC. J., 6 (2014) (Austl.).

Gerrard G, Thompson R., *Two Million Cameras in the UK*. CCTV image, 2011, 42(10): e2 (U.K.).

McCahill M, Norris C. CCTV in Britain. Center for Criminology and Criminal Justice-University of Hull, 2002: 1-70, 8 (U.K.).

Armitage R, Smyth G, Pease K, *Burnley CCTV evaluation*, Surveillance of public space: CCTV, street lighting and crime prevention, 1999, 10: 225-50 (U.K.).

Best-Rowden L, Han H, Otto C, et al. *Unconstrained face recognition: Identifying a person of interest from a media collection*, Information Forensics and Security, IEEE Transactions on, 2014, 9(12): 2144-2157 (U.K.).

Mu, Enrique and Stern, Howard A., A Structured Stakeholder Self-Identification Approach for

the Deployment of Public Information Systems: The Case of Surveillance Technology in the City of Pittsburgh, 23 J. INFORM. TECH. MGMT, 50 (2012).

Germain S, Dumoulin L, Douillet A C. *A prosperous 'business'*. *The success of CCTV through the eyes of international literature*, 11(1/2) SURVEILLANCE & SOC'Y, 134 (2013).

Goold B J, Public area surveillance and police work: the impact of CCTV on police behavior and autonomy. 1(2) J. SURVEILLANCE & SOC'Y, 191 (2003).

Cao L, Hou C, *A comparison of confidence in the police in China and in the United States*, 29(2) J. CRIM. JUS., 87 (2001).

Ditton, J. *Crime and the City: Public attitudes towards open-street CCTV in Glasgow.* 40 (4) BRITISH JOURNAL OF CRIMINOLOGY, 692 (2000) (U.K.).

Ho Shah R, Braithwaite J, *Spread too thin: Analyzing the effectiveness of the Chicago camera network on crime*, 14(5) POLICE PRAC. & RES., 415 (2013).

ness, T. and Charman, E., *Closed circuit television in public places: its acceptability and perceived effectiveness.* POLICE RESEARCH GROUP CRIME PREVENTION UNIT, 35 (1992) (U.K.).

Hempel L, Töpfer E, *The Surveillance Consensus Reviewing the Politics of CCTV in Three European Countries*, 6(2) EUROPEAN J. CRIM., 157 (2009).

Finn, R. and M. McCahill. *Representing the Surveilled: Media Representations and Political Discourse in Three UK Newspapers*, POL. STUD. ASS'N CONF. PROC., 2 (2010).

Marx, G. T., *What's New About the 'New Surveillance'? Classifying for Change and Continuity*, SURVEILLANCE AND SOC'Y, 9 (2002).

R. Tang. 2002. *Approaches to Privacy – The Hong Kong Experience*. (citing from Yao-Huai L. *Privacy and data privacy issues in contemporary China*, 7(1) ETHICS AND INFORMATION TECHNOLOGY, 7, 12 (2005) (China).

## Books, Reports and other Non-periodical Materials

DANIEL J. SOLOVE, NOTHING TO HIDE 100 (2011).

NIETO M, JOHNSTON-DODDS K, SIMMONS C W., PUBLIC AND PRIVATE APPLICATIONS OF VIDEO SURVEILLANCE AND BIOMETRIC TECHNOLOGIES 3-4 (California State Library, California Research Bureau) (2002).

WELSH B C, FARRINGTON D P, CRIME PREVENTION EFFECTS OF CLOSED CIRCUIT TELEVISION: A SYSTEMATIC REVIEW, Home Office, (2002) (U.K.).

Goold B J, CCTV and Policing: Public area surveillance and Police Practices in Britain, Oxford University Press, (2004).

PARKINS, GARRY, ET AL., NATIONAL CCTV STRATEGY, HOME OFFICE, (2007) (U.K.).

NORRIS, C., *The success of failure: Accounting for the Global Growth of CCTV*. In: ROUTLEDGE INTERNATIONAL HANDBOOK OF SURVEILLANCE STUDIES, 258 (eds K.S. Ball, K.D. Haggerty and D. Lyon. London: Routledge, 2012).

WALTON, G. (2001), CHINA'S GOLDEN SHIELD: CORPORATIONS AND THE DEVELOPMENT OF SURVEILLANCE TECHNOLOGY IN THE PEOPLE'S REPUBLIC OF CHINA, (2001).

ARGOMANIZ J, GILL M, BRYAN J, PUBLIC ATTITUDES TOWARDS CCTV: RESULTS FROM THE PRE-INTERVENTION PUBLIC ATTITUDE SURVEY CARRIED OUT IN AREAS IMPLEMENTING CCTV, (Home Office, 2005).

ARGOMANIZ J, GILL M, BRYAN J, PUBLIC ATTITUDES TOWARDS CCTV: RESULTS FROM THE PRE-INTERVENTION PUBLIC ATTITUDE SURVEY CARRIED OUT IN AREAS IMPLEMENTING CCTV, (Home Office, 2005).

LYON, D. SURVEILLANCE SOCIETY. MONITORING EVERYDAY LIFE, (Buckingham: Open University Press 2005).

BIGO, D. *Security, Exception, Ban and Surveillance*. In THEORIZING SURVEILLANCE: THE PANOPTICON AND BEYOND, 46 (D. Lyon ed., Uffculme: Willan. 2006).

LEVESLEY T, MARTIN A, BRITAIN G. POLICE ATTITUDES TO AND USE OF CCTV, (Home Office, 2005) (U.K.).

HOME OFFICE, SURVEILLANCE CAMERA CODE OF PRACTICE, (2013) (U.K.).

COMMISSION ON ACCREDITATION FOR LAW ENFORCEMENT AGENCIES, THE 5TH EDITION OF CALEA'S STANDARDS FOR LAW ENFORCEMENT AGENCIES MANUAL, (2005).

PAUL SCHWARTZ & JOEL REIDENBERG, DATA PRIVACY LAW, (1996).

BIANCO, WILLIAM T., AND DAVID T. CANON, *Public Opinion*, In AMERICAN POLITICS TODAY (3rd ed. New York: W.W. Norton, 2013).

LUM C, HABERFELD M M, FACHNER G, ET AL. *Police activities to counter terrorism: What we know and what we need to know*, in TO PROTECT AND TO SERVE, 101 (David Weisburd et al. ed., 2011).

FRED H. CATE, PRIVACY IN THE INFORMATION AGE, (1997).

GOOLD B J., CCTV AND POLICING: PUBLIC AREA SURVEILLANCE AND POLICE PRACTICES IN BRITAIN, (2004).

### Media and Internet Resources

SURVEILLANCE STUDIES NETWORK, A REPORT ON THE SURVEILLANCE SOCIETY, (David M. Wood ed., 2006) (U.K.), <u>http://news.bbc.co.uk/2/shared/bsp/hi/pdfs/02\_11\_06\_surveillance.pdf</u>.

Keith Proctor, *The Great Surveillance Boom*, FORTUNE, April 26, 2013, <u>http://fortune.com/2013/04/26/the-great-surveillance-boom/</u>.

Siegel L, Perry R A, Gram M H, *Who's Watching? Video Camera Surveillance in New York City and the Need for Public Oversight*. A Special Report by the New York Civil Liberties Union, (2006), <u>http://www.nyclu.org/pdfs/surveillance\_cams\_report\_121306.pdf</u>.

Police Executive Research Forum, How Are Innovations in Technology Transforming Policing?, PERF Critical Issues in Policing Series report (2012), <u>http://policeforum.org/library/critical-issues-in-policingseries/Technology\_web2.pdf.</u>

M. Stroud. *In Boston bombing, flood of digital evidence is a blessing and a curse*. THE VERGE, April 16, 2013, <u>http://www.theverge.com/2013/4/16/4230820/in-boston-bombing-flood-of-digital-evidence-is-a-blessing-and-a-curse</u>.

ACLU of Illinois, *Chicago's Video Surveillance Cameras: A Pervasive and Unregulated Threat to Our Privacy*, Feb. 2011, <u>http://il.aclu.org/site/DocServer/Surveillance\_Camera\_</u> Report1.pdf?docID=3261.

Norris, McCahill and Wood, *The Growth of CCTV: a global perspective on the international diffusion of video surveillance in publicly accessible space*, SURVEILLANCE & SOC'Y, 125 (2004), <u>http://www.surveillance-and-society.org/cctv.htm.</u>

Jeffrey Rosen, A Watchful State, N.Y. TIMES, Oct. 7, 2001.

Andrew Parker, Perveillance of CCTV Operator, THE SUN, Feb. 14, 2007.

Spy cameras fail to focus on street crime, THE WASH. TIMES, Aug. 13, 2006.

Jaxon Van Derbeken, 9-month Suspension for Police Officer, S.F. CHRON., Apr. 22, 2005.

Jon Gargis, *Strip Traffic Camera Follows Pedestrians Home*, THE CRIMSON WHITE, Sept. 15, 2003.

Sarah Wallace, *NYPD Housing Surveillance Staffed by Cops Under Investigation*, ABC NEWS, Apr. 23, 2004.

Jonathan Mandell, *Proof of Your Existence, Complete with Bad Photo*, N.Y. TIMES, October 20, 1999.

Murray Weiss, *Bronx Cop Caught in 'Net – Suicide-Video Scandal*, N.Y. POST, June 22, 2004, <u>http://nypost.com/2004/06/22/bx-cop-caught-in-net-suicide-video-scandal/</u>.

*Vids of Students on Arrested Tech's Computer*, 6 NEWS: THE INDY CHANNEL, Feb. 15, 2008, http://www.theindychannel.com/news/education/school-vids-of-students-on-arrested-tech-scomputer.

Brent Champaco, Cameras Catch Kiss, Raising Questions, THE NEWS TRIBUNE, Apr. 26, 2007.

John Files, V.A. Laptop Is Recovered, Its Data Intact, N.Y. TIMES, June 30, 2006.

Heenan Blaikie LLP, *Video surveillance - breach of privacy*, LEXOLOGY, December 7 2010, http://www.lexology.com/library/detail.aspx?g=b0c1da70-e8be-4c4e-9469-780a5ca14b5e.

Clive Norris & Gary Armstrong, *CCTV and the Social Structuring of Surveillance*, 10 CRIME PREVENTION STUDIES, 162 (1999), http://www.popcenter.org/library/CrimePrevention/Volume\_10/06-NorrisArmstrong.pdf.

Jim Dwyer, New York Police Covertly Join In at Protest Rallies, N.Y. TIMES, Dec. 22, 2005.

Marc Jonathan Blitz, *Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Tracks Image and Identity*, 82 TEX. L. REV. 1349, 1359 (2004), <u>http://works.bepress.com/marc\_jonathan\_blitz/15</u>.

New York City, *N.Y.C. Police Dep't Pub. Sec. Privacy Guidelines* (Apr. 2, 2009), <u>http://prtl-prd-web.nyc.gov/html/nypd/downloads/pdf/crime\_prevention/public\_security\_privacy\_guidelines.pdf</u>.

Thomas J. Nestel, III, *Using Surveillance Cameras to Monitor Public Domains: Can Abuse Be Prevented?* (March 2006) (unpublished M.A. dissertation, Naval Postgraduate School), <u>https://www.hsdl.org/homesec/docs/theses/06Mar\_Nestel.pdf&code=c652f57a750279b26159c07</u> <u>bb6989fd6.</u>

Jennifer Valentino-Devries, *Document Trove Exposes Surveillance Methods*, WALL ST. J., Nov. 19, 2011, <u>http://www.wsj.com/articles/SB10001424052970203611404577044192607407780</u>.

Wood D M, Ball K, Lyon D, et al., *A report on the surveillance society*, Surveillance Studies Network, (2006) (U.K.), <u>https://ico.org.uk/media/about-the-ico/documents/1042388/surveillance-society-public-discussion-document-06.pdf</u>.

Marianne L. Gras, *The Legal Regulation of CCTV in Europe*, SURVEILLANCE & SOC'Y 217 (2004), <u>http://www.surveillance-and-society.org/articles2(2)/regulation.pdf.</u>

ICO, IN THE PICTURE: A DATA PROTECTION CODE OF PRACTICE FOR SURVEILLANCE CAMERAS AND PERSONAL INFORMATION, (2015) (U.K.), <u>https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf.</u>

C.R.M. 1-99 § 32, <u>http://www.justice.gov/usam/criminal-resource-manual-32-video-</u> surveillance-use-closed-circuit-television-cctv.

AMERICAN BAR ASSOCIATION, CRIMINAL JUSTICE STANDARDS § TECHNOLOGICALLY-ASSISTED PHYSICAL SURVEILLANCE.

http://www.americanbar.org/publications/criminal justice section archive/crimjust standards ta

<u>ps\_blk.html</u>.

Charlie Savage, US doles out millions for street cameras Local efforts raise privacy alarms, THE BOSTON GLOBE, Aug. 12, 2007,

http://www.boston.com/news/nation/articles/2007/08/12/us\_doles\_out\_millions\_for\_street\_came ras/?page=full.

David A. Fahrenthold, *Federal Grants Bring Surveillance Cameras to Small Towns*, WASH. POST, Jan.19, 2006, <u>http://www.washingtonpost.com/wp-dyn/content/article/2006/01/18/AR2006011802324.html</u>.

Sarah Berlin, *Department of Homeland Security funding surveillance on the local level*, BORDC, September 19, 2013, <u>http://www.bordc.org/blog/department-homeland-security-funding-surveillance-local-level</u>.

Joe Wolverton, II, J.D. *Federal Grants Enable Increased Surveillance by Local Gov't*, THE NEW AMERICAN, 15 October 2013, <u>http://www.thenewamerican.com/usnews/item/16737-federal-grants-enable-increased-surveillance-by-local-govt</u>.

Smith, E. A. and Lyon, D, *Comparison of Survey Findings from Canada and the USA on Surveillance and Privacy from 2006 and 2012*. 11(1/2) SURVEILLANCE & SOC'Y 190 (2013). <u>http://www.surveillance-and-society.org.</u>

## Non-English Materials

Guanyu Jiaqiang Gonggong An'quan Shipin Jiankong Jianshe Liangwang Yingyong Gongzuo de Ruogan Yijian (关于加强公共安全视频监控建设联网应用工作的若干意见)[Several Opinions on Increasing Efforts to Establish and Network Public Security Video Surveillance], Fa Gai Gao Ji (发改高技) [2015] 996 Hao(号) http://www.ndrc.gov.cn/zcfb/zcfbtz/201505/t20150513 691578.html (China).

Liu Chengbo(刘成波), Gonggong Changsuo Shipin Jiankong de Falv Guizhi—uizYinsiquan Baohu wei Shijjiao(公共场所视频监控的法律规制——以隐私权保护为视角) [The Legal Regulations of Video Surveillance in Public Places: From the Perspective of Privacy Protection.] 18 (2013) (M.S. thesis, Jilin University.) (China).

Gong'an Bu Jiang Jiada Shipin Jiankong Xitong Fugai Huo Quan Hangye Dailai Lihao.(公安部 将加大视频监控系统覆盖或全行业带来利好)[The Ministry of Public Security will enhance the coverage of CCTV, may benefit the whole industry], Zhengquan Shibao Wang (证券时报网), Nov. 7, 2014, <u>http://kuaixun.stcn.com/2014/1107/11835126.shtml</u> (China).

Ye Zusheng(叶竹盛), Gong'an Juzhang de Quanli Chang (公安局长的权力场)[The power games of the Police Chief], 5 Renmin Wenzhai (人民文摘,第5期) (2012). <u>http://paper.people.com.cn/rmwz/html/2012-05/01/content\_1059394.htm</u> (China).

Yang Jianguo (杨建国), Lun Shipin Jiankong de Fanzui Yufang Gongneng ji Fanzui zhengcha Jiazhi (论视频监控的犯罪预防功能及犯罪侦查价值)[CCTV's Crime Prevention Functions and Crime Investigation Values], Fanzui Yanjiu (犯罪研究), 66, 2011年第1期 (China).

Zhang Lianhan (张潋瀚), An Empirical Study on the Operational Mechanism of Skynet Surveillance (天网监控运行机制实证研究), (2014) (unpublished M.A. Thesis, Sichuan University) (China).

Chang Jian, Zhang Chengming (常健、张成明), Shanxi Gongan Jiguan Yinian Jiezhu Jiankong Shipin Po'an 13321 Qi. (山西公安机关一年借助监控视频破案13321起), Huanghe Xinwen Wang (黄河新闻网), Feb. 9, 2015, <u>http://law.sxgov.cn/content/2015-02/09/content\_5550768.htm</u> (China).

Huangpu Gong'an Fenju (黄埔公安分局), 1.6 Wan Ge Shipin Jiankong Dian Quan Fugai, Qunian Huangpu Jinfang Kantu Po'an 703 Zong.(1.6 万个视频监控点全覆盖, 去年黄埔警 方看图破案 703 宗)[16000 cameras cover, the police of Huangpu has solved 703 cases last year], Fenghuang Wang (凤凰网), Jan. 19, 2015, http://gz.ifeng.com/zaobanche/detail 2015 01/19/3449235 0.shtml (China).

Unpublished materials. Ma Jinghua, Zhang Lianhan (马静华, 张潋瀚), SiChuan Shuangliu and Hongya public opinion surveys. (四川省双流县、洪雅县公众意见问卷调查分析) (on file with author) (China).

Ma Deyong (马得勇), Zhengzhi Xinren Jiqi Qiyuan—iyuaYazhou 8 Ge Guojia he Diqu de Bijiao Yanjiu (政治信任及其起源——对亚洲 8 个国家和地区的比较研究) [Institutional and Cultural Factors of Political Trust inEight Asian Societies]. 5 Jingji Shehui Tizhi Bijiao (经济社 会体制比较), 79 (2007) (China).