Situational Surveillance Control

By

Vincenzo Antonio Sainato

A dissertation submitted to the Graduate Faculty in Criminal Justice in partial fulfillment of the requirements for the degree of Doctor of Philosophy, The City University of New York

2009

This manuscript has been read and accepted for the

Graduate Faculty in Criminal Justice in satisfaction of the

dissertation requirement for the degree of Doctor of Philosophy.

Date	Dr. Patrick O'Hara Chair of Examining Committee
Date	Dr. Karen Terry Executive Officer

Ric Curtis

Bilal Khan

Supervision Committee

THE CITY UNIVERSITY OF NEW YORK

Abstract

Situational Surveillance Control

By

Vincenzo A. Sainato

Advisor: Professor Patrick O'Hara

This research considers the adoption, design, implementation, and oversight of digital surveillance technologies in the daily and critical functions of the Belleville Police Department. This agency has custom designed and implemented a digital surveillance and data management system which has since been adopted by forty police departments across its state—including the State Police; moreover, Belleville's data systems interface with the principal national and state-level criminal justice databases, as well as with data sources external to the criminal justice system. The agency provided, to the extent permissible by law, complete access to the agency's employees and systems, as well as all available historical data and records relating to the creation and development of the system. The researcher collaborated with the agency's employees in an extended ethnographic study of their digital surveillance technologies and processes in order to empirically assess associated potential and actual harms, issues, problems, and vulnerabilities. This study concludes by proposing ways that harm reduction models, such as Situational Crime Prevention, can be applied to digital surveillance technologies to improve oversight and accountability.

Acknowledgements

Many people have made this document possible

My wife, Suzanne, has been exceptionally supportive even as nights and weekends were lost to writing and teaching. I had pledged to her that I would complete my doctoral studies in three years, a fair amount of time for an accomplished attorney to have her husband pursue doctoral studies and the associated modest income. I kept my promise, even as I took three to four classes a semester while teaching and serving as a research assistant on major projects. My mom, to whom I also owe a major debt for all my education, was quick to point out the raccoon-like circles around my eyes that resulted. She, and the rest of my extended family across Ohio and Pennsylvania, may not have always understood what drove me to pursue MAs and a PhD after I had 'finished college' but they were never anything but supportive. I thank them for this.

In the doctoral program I have made some very good and dependable friends with whom I could collaborate and commiserate.

Alissa Ackerman was a sounding board for my ideas and never shied from serving as a strong counterpoint, whether the subject was research or politics. She also has tremendous integrity and is remarkably consistent in a world where shifting opinions are the norm. Meghan Sacks was an effervescent and ever-patient friend, who also didn't shy from telling me what she thought when I sought her counsel. Geoff Rad read this document from cover to cover and gave me invaluable feedback. Zach Shemtob is someone whose advice and support I hope to call upon into the future.

John DeCarlo deserves special mention. We first connected when I praised a book about Situational Crime Prevention that I had just finished and he took the very

same book out of his backpack with an air of reverence. John has been a collaborator on articles, and a friend who opened up his home to me when conference paper deadlines loomed. I want to thank him and his wife Katharine and his son Evan for their constant hospitality.

I have also been helped by a wide circle of professors and mentors at John Jay College and at Fordham University. Fordham's Dr. Henry Schwalbenberg recruited me for the Economics and Political Economy program. He encouraged and facilitated my application of econometric and political economy analysis to issues of transnational crime and economic development that served me so well in my doctoral studies.

As a doctoral student, I was offered the opportunity to work on an NSF project on identity technology management in concert with Drs. John Kleinig and Peter Mameli who served as principal investigators for the grant. Much of the work I did, especially with Dr. Mameli, set the stage for this dissertation. With the encouragement of John and Peter, I presented my work on this grant at various regional, national, and international conferences.

At John Jay, Dr. Marilyn Rubin, the MPA Program Director, has also been a mentor and a provider of opportunities. She gave me my first opportunity to teach graduate courses and always made herself available for candid advice and direction. The members of the Public Administration and Economics faculty and staff generally have been tremendously collegial and supportive. In particular, I want to thank Drs. Joan Hoffman and Jay Hamilton who first put the put the 'bug' in my ear about pursuing a PhD.

In 2002 Dr. Mangai Natarajan's introduced me to the concepts of Situational Crime Prevention in her International Criminology class. She guided and encouraged me to pursue graduate study, and has been a valuable mentor throughout.

Dr. Patrick O'Hara, another member of the public administration faculty, just happened to be on a panel where I gave a presentation on national identity card systems and policing and social control in April of 2008. He told me that I was on to something important and that I needed to find a way to shape these issues into a dissertation topic. And thus I gained a dissertation chair and, when the opportunity to get inside a police agency presented itself, this project took off. Pat has been a tireless mentor and his guidance helped make this document possible. He is passionate about what he does, as am I, and he helped me navigate around vexing issues and through seemingly endless drafts to produce what you see here. I thank him for the amazing amount time and effort he devoted to this project.

I also want to thank the faculty who reviewed my proposal and served on my dissertation committee. I value Dr. John Kleinig's high expectations of quality and the integrity with which he pursues and gauges academic research and hope I have absorbed fully his lessons. Dr. Bilal Khan has been a steady force on my dissertation committee with his capacity not only to analyze how organizations manage their technology but also how human factors interact with technical ones in both policing and academe'. Dr. Ric Curtis, who reviewed my proposal and then joined my dissertation committee, helped me shape the methods of this essentially ethnographic study. As one who was trained principally in deductive and probabilistic quantitative analysis, I appreciated all that Ric taught me about inductive and holistic approaches to research. Finally, Dr. Josh

Freilich's careful reading and critical feedback of my proposal and dissertation draft escalated the quality of this document tremendously.

To the employees of the Belleville Police Department, the Police Chief, and the Mayor of Belleville I am grateful. Without their willingness to collaborate and open their doors to my constant probing this document would not be possible.

I am grateful also to Dr. Candace McCoy, my advisor during my first year of Doctoral studies, for encouraging, and naming, my "panoptic" approach to issues. So this work is, thanks to her, the synthesis of various professional and academic experiences. She enabled me to avoid becoming over-specialized in a narrow area of criminal justice where the real possibility is that an individual understands more and more about less and less, even as the problems of crime, deviancy, punishment, security, surveillance, and many others require integrated analysis across the spectrum of disciplines in the social sciences, as well as in arts and science.

Finally a word about John Jay College of Criminal Justice, which houses the City University's Doctoral Program in Criminal Justice. John Jay is an institution where criminal justice research does cut across disciplines and methodological approaches, as does this dissertation, which might not have been possible anywhere else. From day one I was given the freedom to identify opportunities for teaching, service, and scholarship and to pursue them as far as I could take them. No one pushed me towards research that fit their own agenda—not that that would have worked. Instead I feel that I have earned my degree from a premiere institution of criminal justice learning where an acceptance of research diversity is its enduring strength.

Table of Contents

List of tables

List of Illustrations

Chapter 1: Overview

This case study considered the adoption, design, implementation, and oversight of digital surveillance technologies in the daily and critical functions of the Belleville Police Department; moreover, this study asked whether applying Situational Crime Prevention [SCP] concepts and strategies can effectively reduce potential harms by guarding against agency, employee, or contractor abuse of these digital surveillance systems.

The ubiquity of digital surveillance technologies and networks woven into the basic fabric of our everyday lives has resulted in what Lyon has termed "Surveillance Societies" (1994). The critical characteristics include a dependence on communication and information technologies for administrative and control processes (Lyon, 2002). Though the intention of the surveillance is most often benign or, at least, socially beneficial, paradoxes and arguments abound regarding surveillance societies' genesis and direction. To some, it is the logical progression of history[1], to others it is an overt attempt from those in power to amass more power and control.

Simply put, there is no accepted orthodoxy.

But all agree, you are being *surveilled*- from the French verb meaning "watched over". For this study surveillance is defined as " the collecting or processing of personal data, whether identifiable or not, for the purpose of influencing or managing those whose data has been garnered" (Lyon, 2002). This is neither necessarily pejorative nor dystopic.

---

[1] Or perhaps 'rational' progression See (Parenti, 2003)

As Lyon (2002b) argues, surveillance comprises elements of *both* 'control' *and* 'care'. These are, according to him, the 'two faces of surveillance'. Surveillance is not about any one specific technology, rather, it concerns the collection of technologies and the effects those technologies have on social order and the political economy[2].

The idea that police are *surveillers* is not something that is necessarily 'new' (Lyon, 2007a, 2007b). In many societies the police play a unique and distinctive dual role that subsumes providing both 'care' and 'coercion'. Police provide 'care' for society by being the first to respond to a call for emergency or solving a crime. The police are also a coercion agent- being the most visible instrument of the government's monopoly on the legitimate use of force. Traditional examples of police coercion include overt action such as interrogating and jailing of suspects as well as subtle displays of latent force as exemplified by routine foot patrols. Arguably these 'coercions' could be seen as 'care'- depending on one's perspective. In essence, police play roles that are both useful and necessary while embodying coercion and care in varying degrees.

Digital surveillance

Digital surveillance technologies [DSTs] broadly refer to a diverse spectrum of instruments, applications, structures, networks, hardware, and software. The key characteristic is that these technologies make it possible to acquire, share, or otherwise process data as part of a surveillance scheme. Technologies, in the DST context, refers to

---

[2] For a more complete discussion on the notion of the technology 'assemblage' (See Deleuze & Guattari, 1987; Haggerty & Ericson, 2000).

digital mechanisms, alone or concert, which permit the "focused, systematic, and routine attention to personal details for the purposes of influence, management, protection or direction"(Lyon, 2007a) of groups or individuals.

Digital surveillance technologies can be overt, such as a CCTV camera recording the patterns of usage at train station or a database containing traffic violations. DST's can also be subtle- serving a legitimate function but yielding data that can facilitate the surveillance of individuals or groups. For example, a loyalty card from a drug store makes it possible for an individual to obtain points that can be turned into future discounts on desired goods; however, this form of surveillance allows others to form an opinion of whom they perceive us to 'be' based-on our collected record of what, when, where, and how much we purchased.

Whether overtly or indirectly deployed as DST's, systems of computing that generate or analyze data have rapidly become an element in our everyday lives. Greenfield (2006) describes the extent of the DST's reach- literally 'everyware'. In increasing and pervasive ways data is being acquired and put to use. Thus, the *everyware* intrusion into our daily lives by DST's has created great conveniences and brought new risks.

Many are familiar with identity theft concerns that come along with the 'everyware' conveniences; however, Rule(2007) contends that the real problem does not lie with the illegal activities of the few but the legal activities of the many. By this he means that governments and private entities conduct privacy eroding actions as part of their normal and routine functioning. This erosion, he argues, includes the accumulation, application, and disbursement of individual's private data. Rule(2007) convincingly

shows that we all contribute to the accumulation, application, and disbursement of our private data by our *frequently unguarded sharing of information with various individuals and institutions and paying little attention to what is done with the data*. In sum:

- Information is currency;
- People eagerly exchange information for a perception of convenience and security; and
- The legal acquisition and use of personal data by entities yields opportunities for illicit or illegal uses by the same organizations and their agents.

Police agencies, at all levels of government, use digital surveillance technologies to collect, share, transfer and analyze vast quantities of data. Since 9-11 the use of digital surveillance technologies has intensified as police agencies are increasingly putting resources toward advanced digital surveillance systems and technologies (Ball & Webster, 2003; Lyon, 2003a; Monahan, 2006; Webb, 2006)[3]. From 9-1-1 systems and investigations to booking suspects, police agencies have systematized and infused these technologies into all areas of routine and critical police functions. The type of information directly collected by police, or otherwise acquired, has the potential to yield positive gains- such as increased agency efficiency or solved cases; however, misuse of data can cause real or perceived harms to both civil liberties and human rights. For example, an offender is arrested and provides another's ID as their own which results in

---

[3] For a review of policing and surveillance technologies, pre 9-11, (See Ericson & Haggerty, 1997; Gilliom, 2001; Lyon, 1994; Marx, 1988; Nunn, 2001)

that third-party having their record tainted with another's crime(s)(See "Wilson v. City of Louisville, Ky," Nov. 11, 1998); or the situation where someone is arrested and held due to negligent digitized record keeping by an employee (See "Arizona v. Evans," 1995). In extreme cases we see the potential to systemically employ surveillance data to facilitate genocide (Fussell, 2001; Power, 2002).

The misuse, purposeful or not, of collected information by government agents is neither new nor innovative. What is different now is the capacity to use the ubiquitous and proliferating DST's to acquire, transmit, and store the data at a speed and scale that has never before existed. Furthermore, these systems are increasingly at risk for improper access and/or uses by agencies, their agents, and contractors (Inspector General, 2006).

In short, government entities are increasingly reliant on networked surveillance technologies linked to digital databases that:

- Contain vast quantities of micro-level data which are obtained from a variety of sources including private, public, and non-profit organizations;
- Are increasingly central in the critical and routine functioning of the agencies;
- Are highly vulnerable to errors emanating from data conjoined from multiple sources;
- Have limited oversight mechanisms to control or prevent harms associated with the valid/legal 'everyday uses' of DST's;
- Have limited oversight mechanisms to control or prevent harms associated with the illegal/illicit uses of DST's;

- Rely largely on oversight mechanisms designed for after-the-fact responses to problems; and therefore,
- Have few built-in mechanisms to proactively prevent abuses of the DST's or associated systems.

One application of 'everyware surveillance' employed by law enforcement entities in the US are warrantless *demands* put on private entities (such as banks and internet service providers) for data from their clients' files. And these demands have not always resulted in the demanding agency following the legal or ethical constraints with respect to their use of data. For example, a 2007 investigation by the DOJ Inspector General found "…widespread and serious misuse…" by the FBI in documenting and following basic procedures in using it's investigative powers to apply for National Security Letters [NSL] to obtain and scrutinize the financial data, travel records and telephone logs of thousands of U.S. citizens and residents (Inspector General, 2007).

While the FBI has been a frequent target for derision, insufficient oversight and accountability of digital surveillance systems have created many opportunities for abuse by law enforcement agencies or their employees, both in the US and abroad (Altimari, 2006; Laurant, 2003; O'Harrow, 2005; Webb, 2006; Winnett & Swaine, 2008).

Oversight of digital surveillance systems

Oversight and accountability has not kept pace with the rate of change caused by the adoption of new technologies. In many respects current regimes of oversight are *post-*

facto, poorly-planned and fragmented (Friedman, 1997; Goldsmith & Lewis, 2000; Thompson, 2000) or non-existent (Inspector General, 2007).

Typically, government agencies and their systems are designed around their functional or procedural goals (Sparrow, 2008). The standard model of modern law enforcement traces its roots to the 18th century techniques of Fielding and his Bow Street Runners whose primary focus was on the rapid response to reported criminal events (Emsley & Shpayer-Makov, 2006). Since the 1980's there has been a tremendous shift as law enforcement agencies begun to put a priority on risk reducing or preventive models such as Problem-oriented Policing [POP] (Herman Goldstein, 1990; Sparrow, Moore, & Kennedy, 1990). Policing models such as POP advocate for the infusion of a diversity of approaches including an emphasis on the use of digital surveillance technologies (Ericson & Haggerty, 1997). Thus, law enforcement agencies are adopting new stratagems and surveillance technologies but new modes of oversight of those technologies are not keeping pace.

Post-facto approaches to police oversight with respect to law enforcement surveillance systems, data management and digital technologies are the norm. In networked digital environments oversight should be overtly re-cast to delimit and deter harms rather than react to their occurrences (Sparrow, 1994, 2008).

Theoretical and empirical foundations for designing protocols for oversight whose fulcrum is in a harm-elimination or a prevention-oriented approach is found in the Situational Crime Prevention [SCP] literature (R. Clarke & J. E. Eck, 2006; Sparrow, 2008). A variation on the POP-theme, SCP has traditionally been used by law enforcement to develop protocols for preventing crimes in traditional settings such as

open-air drug markets. That said, recent scholarship has argued that this approach can be used in 'cyberspace' (Clarke & Newman, 2006; G. R. Newman & Clarke, 2003); however, no specific protocol has been elaborated using SCP as a tool for 'preventative oversight' *within* organizations[4]. Additionally, SCP literature tends to focus on exogenous prevention of deliberative abuse rather than the harms that can come from the 'everyday uses' of the systems. This research argues that harm reduction protocols can be employed during the proposal, design, and implementation phases of new systems[5].

Importantly, *digital surveillance technologies and software can only do what their designers program them to do*- this is done through the lines of code that tell the computer what operations to undertake; moreover, software is dynamic as, over time, different versions and iterations are coded, recoded, and eventually implemented. Thus, fundamental assumptions guiding this research are:

1) Elements that can be built into the design and operational maintenance processes are key to assuring either a faithful adherence to legal or regulatory requirements or enabling a willful disregard;
2) Proactive design can control or prevent many of the negative externalities associated with these system; furthermore,

---

[4] That said, Willison (2008) argues that SCP should be used to inform the otherwise atheoretical approaches to Information Systems [IS] security practices. This is discussed below..

[5] This mindset is not unknown to the builders and designers of 'real' space or environments (Crowe, 2003; Design Against Crime, 2003; Tilley, 2005; Western Australia Planning Commission, 2005).

3) Design, from inception, for the software's code (or encoding the data itself) should delimit applications and analysis that does not comport with the legal and/or regulatory code governing law enforcement agencies.

In short, government agencies need to isolate the who, how, when, where, and what when things do go 'wrong' and then develop preventative architecture

Developing new ways, means, and protocols for the oversight of DST's employed by law enforcement presents several challenges. Importantly, there is a limited body of empirical literature that provides the necessary 'behind-the-scenes' accounting of how police agencies use these technologies.

Government reports in the US tend to focus on a specific incident where things have gone, or are going, 'wrong' (Inspector General, 2005, 2006, 2007; Technology And Privacy Advisory Committee, 2004). While useful, these reports provide a very narrow view of law enforcement and DST's. Empirical case studies conducted by social scientists tend to be extremely limited in scope. Especially in the US, and since 9-11, police agencies are understandably averse to outsiders obtaining intimate access to their people or studying the nuances of their daily operations in the surveillance context. Outside of the US, scientists have been able to study police and DST's in very narrow contexts. For example, there is no shortage of papers out of Europe concerning policing and CCTV's (Benjamin J. Goold, 2003; B. J. Goold, 2004; Sætnan, Lomell, & Wiecek, 2004).

At present, neither official government reports nor empirical studies by social scientists provide insight into law enforcement and the ubiquitous and pervasive 'everyday' uses of DST' or the efficacy of harm-reducing oversight mechanisms.

This study

For this study the researcher conducted an embedded case study to explore the entire array of digital surveillance technologies in a law enforcement agency. The purpose was to understand how DSTs were employed in the routine and critical functions of policing; but, beyond that, how these technologies were chosen and implemented, how the organization shaped itself around the technologies, and importantly, the current state of practice with respect to the safeguarding citizen information from agency or employee abuse(s).

This study includes an extended ethnographic field study in Belleville, Connchusetts with the Belleville Police Department [BPD]. The BPD was selected for this study due to a number of reasons:

The BPD is a model agency because it was the first Connchusetts law enforcement agency to implement a third-party digital surveillance system designed to integrate the routine and critical functions of the police, fire, and EMS into a common interface; moreover, the current BPD chief was the lead software designer of that system and now that system has been adopted by over 40 Connchusetts agencies, including the Connchusetts State Police. Additionally, the BPD employs other 'home-grown' digital surveillance technologies as well as customized third-party and web-based data mining or

analysis applications. In addition to their localized surveillance technologies, the BPD employs the ‘standard set’ of state and federal digital surveillance systems.

In June of 2008 the researcher provided the executive officers of the BPD with a proposal outlining his intended research. At that time the BPD was considering hiring a third-party consultant to assess and audit their data systems. They had added so many features, functions, and new applications since 2001 that no one had a complete view of all of their data collection(s), surveillance, and data management technologies. The BPD invited the researcher to collaborate with their employees and facilitate an assessment of their complete system with the agreement that the researcher would, in turn, be able to use the findings for this study.

The purpose of this embedded case study was to explore a typical police agency in its everyday use of digital surveillance technologies. By working in direct collaboration with the agency and its employees and with the approval of their senior leadership, the researcher, through his continual presence, was able to gain a complete understanding of how the agency chose, implemented, and employed digital surveillance systems for both the routine and critical functioning of the agency. The researcher’s training as a social scientist and his extensive experience in the design and implementation of DSTs provided him with unique insight that made it possible for this project to be conducted efficaciously.

This research yielded a thorough understanding of DSTs in action and the mechanisms to control or prevent the negative externalities associated with the use of the DSTs employed by the Belleville Police Department (BPD). The knowledge generated from this inquiry, as detailed in later chapters, will afford new theoretical and practical

insights, and inform practitioners on how better to govern the design and use of digital surveillance and data systems.

This inquiry was guided by the research questions outlined below:

- In what ways does the BPD use digital surveillance technologies/systems in its critical and routine functions and activities?
- In what ways does the BPD integrate new systems to ensure that the concerns of oversight are taken into account during the planning, design, and implementation process?
- In what ways does the BPD employ oversight mechanisms to control or prevent harms in the routine and lawful operation of these systems?
- In what ways does the BPD employ oversight mechanisms to control or prevent harms from employee abuse and misuse of these systems?
- In what ways are citizens at risk due to the illegal or illicit uses of these systems by the BPD or its agents?
- Can a harm-reduction and preventative mindset such as the SCP approach lead to the design of policies and protocols that better guard against externalities and, if so, what specific protocols or policies could be employed?

This study contributes to existing literature in several important ways:

- First, SCP interventions are normally employed by police agencies to control or prevent unwanted behaviors within the community and not within the police agency itself.
- Existing literature and case studies on SCP have almost exclusively been applied to "real world" space (i.e., open-air drug markets, vandalism in train stations, etc.): to date, no one has conducted an empirical case study analysis of an actual digital surveillance and data system within the context of the SCP framework.
- This study focuses on the regulation of behaviors and uses of digital surveillance systems by "everyday" users - those who are *inside* the system and permitted to use it - whereas previous efforts to bring SCP to digital environments have primarily focused on "outside" offenders (or hackers) who attack data management systems from the outside.
- Fourth, to complete this research an extensive case study was conducted of a police agency and its use of digital surveillance technologies. This is *highly* unusual - police agencies are extremely averse to outsiders obtaining access to their people or systems in the surveillance context.
- Fifth, this research found that at least 3 of the 5 categories of SCP techniques were directly applicable in the DST environment and explicitly contribute to increasing the oversight of police and their use of these technologies.

- Sixth, this research evolved and applied a protocol for inquiry of DSTs that can be used to evaluate the DSTs using the principles and concepts of SCP.
- Seventh, the findings suggest that some of the key conclusions in the existing canon of sociological-based inquiry into surveillance systems and law enforcement may have overlooked an important point regarding the increased capacity to scrutinize and control the behaviors of law enforcement itself vis-à-vis DSTs.
- Eighth, this research found that the presence of DSTs does not diminish the professional and social networks among law enforcement personnel and between jurisdictions and agencies.

Throughout this study, linkages between computing capabilities, the administration of law enforcement, surveillance technologies, and oversight thereof are primarily viewed through a combination of criminological and sociological concepts. These concepts are outlined in Chapter 2. This leads, in Chapter 3, to a review of the methods employed during this research. Chapter 4 provides a thorough description of the setting. This segues into Chapters 5 and 6, which includes a detailed accounting of the development of DSTs in Belleville starting in the 1970s and a thorough explication of the current status of the DST network that is currently employed. Lastly, Chapter 7 presents discussion and concluding comments.

Chapter 2: Literature review

Much has been written about the technical, social, and political processes by which societies are becoming increasingly *surveilled*. There are competing views about this higher level of surveillance and what it means. These views cross ideological and political lines: they range from seeing it as a new phenomenon that will result in dystopian nightmares, as merely a continuation of existing trends or somewhere in-between[6]. What can be said is that the modernization and globalization of societies has resulted in the creation and distribution of digital systems which allows for massive stores of data on people and the lowering of barriers within and between state and corporate entities with respect to sharing and exploiting that data.

Technology has facilitated the "deepening integration of societies" by providing the means by which systems (regulatory, economic, etc.) can be linked and made more efficient. Typically, these open and dynamic technological systems are also characterized as being capable of sustaining dramatic innovations without their balance being threatened. Modern societies have interlinked digital surveillance and other technology networks as a means of mediating exchange and coordination amongst the participants. The networks are so ubiquitous that they are more likely to be noticed when they are not available. Two obvious examples are the cellular telephone and email. Many people don't think twice about being able to walk down New York's 5th Avenue while speaking on a

---

6

cell phone with a friend in Tokyo or typing a memo to a colleague in Australia while sitting comfortably in a Viennese coffee shop. Meanwhile, these networked technologies have changed the way we interact, as well as our social expectations of others. Castells (1996) refers to this phenomenon as the "network society."

To Castells (1996), the network society is not about creating new kinds of relationships; rather, it is a way of mediating relationships. For example, traditional one-way broadcast media has reached a new level of dynamism with the popularity of radio talk shows, internet blogs, podcasts, and other mediated forms. This explosion of content suggests that the chief currency of the network society is the data on the network(s). However, Castells argues that this is not the case; rather, the networks themselves are the key currency. Castells posits that the real power is in the control over the switches and nodes that *direct* the flows of data. In his words, "…the power of flows takes precedence over the flows of power." He explains that the reality of multiple overlapping networks becomes the critical source for shaping, directing, guiding, and misguiding public opinion. Thus, the means for creating dynamic efficiencies in information transmission also has the potential to yield *significant* controls on society[7,8].

The data and the networks have a symbiotic relationship. The ultimate usefulness for each is dependent on the other. Therefore, data *is* important, as without data the

---

[7]Disturbing examples of overt controls appear to be all too frequent in modernizing China, but apparently no one is surprised .

[8]This is especially true for vulnerable populations who tend to have greater dependency on systems that both provide and inherently control. Gilliom's in-depth account of the rural poor in America illustrates this reality, as well as how the "system" is subverted; moreover, both he and Parenti show that in the U.S., historically, this is not a new phenomenon, *per se*, but the pervasiveness and efficiency of the control is.

networks would have no purpose, since the utility of the network(s) is a function of its ability to efficiently transport data from point A to B. On the other hand, the vast collection of fragmented networks on which data resides recombines that data in so many ways and for so many purposes that no one entity can effectively exercise control.

Data bodies

Digital networks have mediated the dynamic changes in personal and society-level relationships. Technologies - surveillance and otherwise - have facilitated and mediated relations as societies have become larger and people less known to each other. Developments such as individual seals and signatures were created to act as our surrogates. As nation-state affiliation became more critical, devices such as national ID cards and passports were developed to affirm the affiliation and identity of an individual.

Over time, our physical bodies have become less important to exchanges as our digitized "data bodies" have become more critical. "Data bodies" are our representatives in the digital systems and networks and they are derived from the "assemblage" of data that exists about who we are, what we do, how we do it, and more. The data body exists in the ether and yet it is always "with" us. To prove this, one only has to open his wallet and see the combination of loyalty, bank, gym membership, work ID, driver's license, medical insurance, credits cards and more contained therein. These are "active" means of obtaining behavioral data on us. The cards are physical manifestations of us - who we are and what we do and, *ceteris paribus,* they are fairly benign creators of efficiency and utility. There are also "passive" surveillance systems such as the closed-circuit television (CCTV) in our college library, the speed sensors in the pavement, web filtering on our

computers at work, and many others. These "passive" systems collect data that is typically inferential and distant. However, conjoining the behavioral information collected by both "active" and "passive" means makes it possible to create a detailed representation of "who" we are: our "data body."[9]"

Our data bodies are not subject to physical time-space constraints. Our data bodies precede, follow, and show up with us. Many data body representations of us are "running" around simultaneously, and we have limited control over when and where a snapshot of our data body is taken and to what degree one or another snapshot accurately represents us.

The data body concept is not essentially pejorative or normative. Data bodies, through the networks on which they exist, represent us when we cannot represent ourselves, and we frequently like that. For example, an email from *Amazon.com* suggesting that a customer who purchased David Lyon's previous texts is likely to be interested in his new one… at a "deeper than usual" discount. Timely reminders and targeted discounts are clearly a function of *Amazon.com*'s understanding of a given customer's data body. The downside of the lack of control over our data bodies can range from the annoying, such as email spam, to the sinister, such as the individual with the excellent credit rating who is refused a loan because he lives in a neighborhood where

---

[9]Los prefers the term "data double," but she also casts it in a larger narrative, having to do with the data representation exceeding in importance the "truth" of the person. This idea is an evolution of her research on surveillance and the "scientific totalitarianism" of 20th century regimes (i.e., Nazi Germany); however, the distinction here is that the "data double" is a necessary step toward unintentional totalitarian effects. In essence, the physical paper "file" is replaced by the digital one. Solove's "digital dossier" is cast in much the same light; whereas, *our* use of "data body" can subsume either "double" or "dossier," but it is not *necessarily* pejorative.

people have been known to default. Given the fluidity of our data bodies and the pervasiveness of networks, the full implications of a given data body snapshot are uncertain.

For Lyon, what is certain is that the concepts outlined above are linked together and create a new surveillance-data-network paradigm, the "Surveillance Society."

The "Surveillance Society"

Digital surveillance is often created to serve socially beneficial purposes. For example, traffic cameras can be used to spot-check for roadway safety. Those same cameras can be networked and connected to specialized software that can "read" and digitally record each license plate number. A passport can be embedded with a chip containing personal and travel data that makes it easier to get through customs. Benign purposes are not guarantees against malevolent uses. The same data can be illicitly acquired from a card or passport in order to steal a person's ID or it can be used by governments or corporations to limit freedoms.

There are numerous paradoxes and arguments regarding the genesis and direction of surveillance societies. Parenti (2003) sees them as the logical progression of history. Others see them as overt attempts by those in power to amass more power and control (Gandy, 1993; Garfinkel, 2001; Garland, 2001; Los, 2004; Marx, 1988, 1992a, 1992b; Norris, McCahill, & Wood, 2004; Stanley, 2004; Stanley & Steinhardt, 2003; Steinhardt, 2007).

Simply put, there is no accepted orthodoxy.

But this much is certain: we are all being *surveilled* (from the French verb meaning "watched over"). Surveillance, for this study, is defined as "the collecting or processing of personal data, whether identifiable or not, for the purpose of influencing or managing those whose data has been garnered." Lyon reminds us that surveillance comprises elements of *both* "control" *and* "care." These are, according to him, the "two faces of surveillance."

Modernized societies are comprised of "Big Brothers" - and millions of little ones - who are watching, sorting, checking, and assessing. These activities are made possible through the free-flow and exchange of data on the network(s). It is these activities that facilitate the emergence of surveillance societies. In turn, the surveillance societies serve as catalysts for societies overtly oriented toward risk assessment and management. The everyday surveillance of individual or aggregate data makes risk-based societies possible. All members of society contribute and participate (to varying degrees) in these systems, which provide considerable social utility. In part, the distancing of relationships creates a paradox as greater intensities of surveillance result in greater demands for privacy[10], which, in turn, leads to an even greater distancing of relationships. This promotes a negative spiral of demand for surveillance that is facilitated by the increased accessibility and economies of scale associated with the necessary technologies.

Given the pervasive and ubiquitous reach of the data acquisition systems and their interwoven networks, the question arises, "Is 'Big Brother' *(really)* watching you?" What appears at first to be a straightforward question belies some inherent complexities

---

[10]These are countered by the proliferation of "social software," where people frequently reveal their intimate thoughts and beliefs or attempt to "live" their fantasy lives. These include blogs, wikis, and metaverses.

regarding concepts substantively shaped in literature and social criticism. As an empirical matter, what Big Brother is doing leads to questions regarding technical feasibility, in addition to notions of privacy and surveillance in the context of the criminal justice system and oversight of that system. *Which brings us to a fundamental line of inquiry for this project: if and when Big Brother (the police) is watching - how do we know that he is doing it in a way that meets either the letter or spirit of the legal limitations on his activities*?

Theorizing surveillance

The amount of empirical quantitative research in the surveillance field is seriously limited[11]. This is not surprising given the nature of the subject matter and the relative newness of the field. The bulk of the digital surveillance canon consists of literature from the past two decades; there are few academic "centers of excellence" for digital surveillance (let alone a school of "thought"). Also, the multitude of influences and backgrounds of researchers (from sociology, economics, law, history, philosophy, political science, and beyond) has resulted in an "earnest fragmentation" or, at least, a panoply of subject matters assessed through a multitude of lenses. As such, grounded theory and quantitative and comparative testing of grounded theories and approaches is

---

[11] The early empirical analysis of Rule (1974) stands apart from much of the current literature. Still prescient today, his case studies focus on five large data systems meant to enforce social control through identification of "rule breakers." Rule asserts that the systems themselves are merely a function of the changes in social scale and, in opposition to Orwell, are not inherently "bad." Nonetheless, they do provide opportunities for abuse and curtailments of political and other freedoms. However, Rule is not emphatic on this either; rather, his greatest criticism is aimed at the private sector.

still over the horizon. There is no unified consensus or grand theory with sufficient explanatory power to explain surveillance, why and when it occurs, and why is it experienced differently in different contexts and societies[12]. Significant swathes of the surveillance literature are devoted to arguments from sociologists that are derived from philosophy (Foucault's Panopticon)[13] and fiction (Orwell's *1984*).[14]

Surveillance theory, criminal justice, and the study of crime

The study of surveillance is a littered landscape of theoretical and topical permutations and applications: there is no obvious and necessary starting point. That said, Lyon (2007) points out three topical areas which historically have had their theoretical paths instilled with surveillance themes and ideas: criminal justice, the workplace, and military power.

The ultimate focus of the proposed research is the oversight of police entities with respect to DST's; however, in identifying the three theoretical paths (criminal justice, military, workplace), Lyon has uncovered a principal issue with what is happening in

---

[12] For a succinct, but thorough, discussion of the different contexts and theoretical themes, see Lyon (2007); for more substantial treatments see Lyon, Haggerty, Ericson and their colleagues .

[13] Coupled with the "assemblage" critique, Haggerty and Ericson provide a robust and thoughtful response to Panoptic dogma.

[14]Commentators who employ the "Big Brother"/sky is falling rhetoric (See Stanley & Steinhardt's re-casting of Big Brother as a "monster," including a monster illustration) tend to undermine their arguments by addressing the nuances and failings of the metaphor.

today's surveillance society. We are seeing a conflation of interests in what once were distinct domains due to the dramatic impact of international and domestic terrorism in democratic societies post-9/11.

The issue of conflating realms is no small point. It could be argued that this is advancing the movement toward more dystopian realities concerning the uses of surveillance today, as well as having unforeseen impacts on traditional crime control theories and methods in the real world. Is this conflation pushing the surveillance envelope beyond legal and ethical boundaries? Indeed, this is the ultimate "big picture" question.

Surveillance themes and notions have been integral to many important developments in criminal justice. Arguably, the criminal justice reforms advocated by Beccaria were about the surveillance of the system itself, and by extension, a form of governance; however, the bulk of relevant criminological concepts are found in the literature regarding social control or crime prevention theories.

Much of the historical theoretical groundwork can be traced to Durkheim's notions of crime and relative deprivation between groups, leading to perceptions of the "other" as a threat to security requiring surveillance; however, modern criminologists have gone beyond and, at least in part, built upon Durkheim's simple (but elegant) ideas.

Scholars from the Chicago School of criminology, particularly Shaw and McKay (1942),[15] used maps overlaid with delinquency data to identify persistently "socially

---

[15]For a historical review of the Chicago School see Beirne (2005). Recent elaborations and developments by Bursik and Grasmick extend and test the model to include forms of formal and informal social controls; however, they don't necessarily use surveillance as a dimension, *per se*, of their model .

disorganized" neighborhoods. Their findings led to the implementation of the Chicago Area and the Boston Mid-city Projects, which were designed to increase informal social controls among law-abiding citizens as a means of discouraging "bad" behaviors and cultural transmission of delinquency. These programs led to the widespread use in the U.S. of community crime prevention programs in the 1960s. Arguably, the application of these ideas can be viewed in two ways. They could lead to inclusive policies that truly bridge the real or perceived divide between those classified as "organized" and "disorganized" groups; however, another concern is that these classifications could be and are being used to justify stricter surveillance and controls on the "disorganized"[16].

Historically, criminological theories have attempted to explain the factors that increase criminality (that motivated people to commit crimes); however, perhaps the most widely tested paradigm, control theory, asks the reciprocal question: "Why *don't* people commit deviant acts?" Inherent in this approach is the notion that humans seek pleasure, and yet, most people do not engage in criminal behavior. Control theorists ask which combination of social, psychological, and psychiatric factors cause the greatest *restraining* influence on individuals. Perhaps the most prominent of the control theories, Hirschi's social bond theory, is based on a model arguing that a combination of family, school, and peer factors can increase an individual's social "bond," or adherence to positive social norms.

Criminological control theories (big "C") are largely designed to explain the individual's choices through the prism of internal self-control, as measured by self-reports

---

[16]For a more complete discussion and a comparative historical analysis of surveillance vis-à-vis criminal justice see S. Cohen (1985).

of the commission of deviant acts. When sociologists speak about social control (little ”c”) and surveillance they are primarily referring to the formalized means of social control whereby citizens and their actions or opportunities are delimited as a way of compelling uniformity (See discussion below on “maximum surveillance societies”). The sociologist considers institutional features that most criminological control theory models do not explain. For example, the control-oriented theories don’t necessarily explain the individual’s self-control in the face of national ID cards, or some other form of institutionally managed surveillance-oriented social control. It is possible that this deficiency may constitute a breach of the paradigm’s constraints; however, this is an empirical question that needs testing. After all, the control models are based on external controls to the individual and clearly, surveillance provides that. In either case, newer paradigms have surfaced which attempt to model the potential offender’s choices and the control of unwanted behavior through environmental controls, such as a surveillance technology.

Control theories can provide a way of assessing acts by street offenders who break the law, as well as by employees whose actions breach data management protocols. However, neither control nor social disorganization theories provide an effective overall paradigm for both the modeling of offender-level behavior *and* institutional oversight[17].

In recent years crime policies and protocols have been more overtly crafted to *prevent* (or control), rather than *understand,* criminal behavior. Neo-classical criminology

---

[17]For example, social disorganization theory does not explain what it is about the culture or institutional designs of agencies that result in poor data oversight.

draws upon a diverse set of ideas[18] to articulate a framework for *preventing crime*. Central to its theme is that crimes (taken here to mean any act legislated as such or *any* undesired behaviors) are a function of opportunities present in the physical environment. This is not a causal relationship but a necessary one. Thus, if the opportunity structure of actual crimes and the environments in which crimes take place can be understood, then crime can be controlled - either through deterrence or by sufficiently delimiting the opportunity itself. Specific crime control and prevention paradigms are derived from the neo-classical doctrine, including Crime Prevention through Environmental Design (CPTED), Defensible Space, and Situational Crime Prevention (SCP).[19]

Understanding DSTs

The previous section focused on the sociological and criminological notions of "surveillance" whereas the following discussion focuses on the digital technologies of DST.

So far this report has used the phrase "digital surveillance technology" (DST) in reference to a diverse spectrum of instruments, applications, structures, networks,

---

[18]These include "classical" urban theory literature on social control through natural surveillance , environment and crime , and environmental opportunities and offender choices which, in total, is viewed through the lens of Chicago School social economic theory .

[19]The details of SCP and its potential as a tool for improving the oversight and accountability mechanisms are outlined later in this document, as are criticisms of crime control and SCP. The purpose of this section is to highlight the point that notions of surveillance are embedded in mainstream and current criminological frameworks.

hardware, and software. This is understandable since the primary goal is to assess the oversight and accountability of police and their usage of DST, rather than to assess DST, per se. That said, the DST concept requires elucidation and clarification.

The central concerns related to DST can be looked at through the prism of data management and control. All DSTs have a common critical thread: digitized data.[20] When all other concepts are removed, digitized data is what is left.[21] Thus, this study's principle concern is the oversight of police entities that use digitally procured or stored data to provide "care" or "control," for individuals and for society as a whole.

From the data technology literature three broad classes of DST emerge: acquisition, sharing, and management.

Data acquisition and sharing

Data acquisition technologies constitute any device that can record, monitor, or obtain and digitize data about our legal, illegal, or illicit behaviors, choices, or preferences. This comprises a virtually endless list that includes credits cards, CCTVs, and iPhones (see Table 1 below). These are the technologies that "capture," alone or in concert with others, the information needed to create, feed, exercise, and procreate our data bodies.

---

[20]Throughout this document "data" is assumed to be digital data, unless otherwise stated.

[21]This use of data subsumes the code and algorithms that comprise all software, as well as the information-based data that is carried or stored.

Table 1: Watching What You Do

TECHNOLOGY	DESCRIPTION	SELECTED PROVIDERS
AT HOME		
"Nanny cams"	Small, easily hidden wireless digital video cameras for monitoring	Nanny Check, Plainview, NY
	children and pets.	Know Your Nanny, North Brunswick, NJ
Infrared	Technology that alerts police to such suspicious thermal activity inside houses,	Monroe Infrared Technology, Kennebunk, ME
surveillance	such as the heat from marijuana-growing equipment.	Sierra Pacific, Las Vegas, NV
ON THE ROAD		
Traffic cameras	Web cameras mounted at high-traffic points; specialized cameras	Axis Communications, Lund, Sweden
	that read plate numbers for law enforcement.	Computer Recognition Systems, Cambridge, MA
Automobile	Electronic toll deduction when users pass through tollgates,	Mark IV Industries, Solvesborg, Sweden
transponders	supported by laser vehicle measurement and axle number detection.	SAMSys Technologies, Richmond Hill, Ontario
Cell phones	Technology that reports a cell phone user's precise location to	Mandatory for all U.S. wireless carriers and cell
	authorities during 911 calls.	phone manufacturers by 2006
AT WORK		
Internet and	Text and data filters that ensure compliance with privacy and	Tumbleweed Communications, Redwood City,CA
e-mail monitoring	harassment laws, and corporate confidentiality requirements.	Clearswift, Theale, UK
Keystroke logging,	Systems that record everything typed into a computer, including	Amecisco, San Francisco, CA
file usage review	e-mail, instant messages, and Web addresses.	NetHunter Group, Tallinn, Estonia
AT SCHOOL		
Web filtering	Software that prevents students from reaching inappropriate Web	N2H2, Seattle, WA
	content.	iTech, Racine, WI
Locator	Bracelets that combine GPS and digital cell-phone signals to locate	Wherify Wireless, Redwood Shores, CA
wristbands	the wearer within 30 meters.	Peace of Mind at Light Speed, Westport,CT
AT THE STORE		
Smart cards	Microchips embedded in plastic cards that carry e-cash, along with	Gemplus, Luxembourg
	driver's license, age and address information, and medical records.	Oberthur Card Systems, Paris, France
Supermarket	Cards with embedded chips or standard magnetic stripes that	Catalina Marketing, St. Petersburg, FL
discount cards	earn member discounts and track shopping habits.	SchlumbergerSema, New York, NY

Source: (Farmer & Mann, 2003)

Acquisition technologies can be divided into two sub-categories, *active* and *passive*. The main distinction between these groups is from the user's perspective. Active technologies are the ones that we directly contribute to by our active and overt use.

Examples of this include Smart Cards, iPods, and cell phones. Passive technologies are ones that we are exposed to (and may not even be aware of), such as web filtering, e-mail monitoring, listening devices, and CCTVs. This is what Lyon refers to as "everyday surveillance" - the "watching" of what we are doing by an expanding network of electronic sentinels.

The term "acquisition" implies a one-way flow or monologue of data; however, the acquisition does not have to be a data monologue from "us" to "it." Nearer to the truth is that there is a dialectic, as these technologies can not only observe and record but also control, direct, influence, and alter our behaviors. One clear example of this is the reduction in prank phone calls that are attributed to Caller ID. Potential offenders, knowing that their number may well be "captured," are deterred by this technology.

Data sharing technologies refer to the networks (and their nodes) that carry and transfer data from point "A" to point "B." These technologies include a vast array of systems and protocols, from copper wires and wireless to laser.

Data Management

Data management technologies permit the storage, sorting, modeling, and analysis of a given dataset that has somehow been acquired. Data management can be broken into two broad sub-classes: databasing and data mining.

Databasing

Databasing (or "data warehousing") refers to technologies that can aggregate, store, and sort massive amounts of digital data. A database is typically a computer that serves as a repository for the data. However, any device that can permanently store information is, strictly speaking, also a database. And, given the storage capacity of everyday acquisition technologies[22] like iPods and cell phones, the lines between these categories have become decreasingly "bright" and increasingly "fuzzy". That said, in this research, databases are those technologies that are expressively designed and organized to aggregate and store digitized data for later retrieval.

The modern development of databases is a fascinating tale that has been outlined elsewhere. What follows is review of some key milestones germane to this study.

Databases originated with a punch-card system that was designed to store and sort information for the U.S. Census in 1890. Garfinkel explains how the initial technical and capacity milestones of databases were in support of government functions; however, many of the innovations themselves come from the private sector. A critical juncture in the development of databases emanates from the public's response to the U.S. government's 1965 proposal to create a centralized data repository for all federal agencies, the National Data Center. Each agency would feed data into a single massive mainframe through a unified network. The plan was that all government agencies would

---

[22]For example, Apple's website boasts that the iPod with the largest capacity, 80GB, can store, in some combination, up to 20,000 songs, 25,000 photos, or 100 hours of video.

have efficient and distributed access to the vast array of digital data collected by the Federal Government on a daily basis.

The early proponents argued that this would defragment the disparate data collections at each agency, streamline government services, and take advantage of technological economies of scale. Others argued that this wave of computerization would threaten civil liberties and "humanity." By the end of 1968, the National Data Center was abandoned.

The decision to scrap the National Data Center resulted in a long-term technological "sea change." At the time, building-sized mainframe computers that stored data on cumbersome magnetic tapes represented the "state of the art." Not economizing the data warehousing and supporting networking into a centralized system meant that database makers needed to develop smaller systems, independent of a network external to the host institution. Garfinkel (2001) argues that this provided the direction for the following thirty years of innovations in speed and size. As capabilities increased and costs decreased, more and more private sector firms began to develop and maintain their own databases. Garfinkel (2001) also explains that the 1960s backlash led to a series of laws and government inquiries intended to assess and limit the privacy threats associated with government databases.

Databases have proven themselves to be efficient at organizing and sorting vast tracks of data. Also, not only the government has found value in taking advantage of the capabilities of databases. Increasingly, large and small businesses are not merely tracking exchanges with their customers, but are attempting to acquire as much detailed information about their clients as possible. One way of accomplishing this is to purchase

or rent information from data aggregators. These are firms who have built what Hardt and Negri call “information empires.” Such “empires” can be constructed through a variety of means, including the collection of public records. The empires also add to their own data service offerings by purchasing data from other collectors. For example, suppose you use a frequent shopper card at the grocery store. The data associated with that account - what you purchased, when, and in what quantities - can be valuable information to some entity. The value most likely comes from the aggregated data, because retailers and marketers want to know (generically) what people “like you” are interested in .

Nonetheless, these data “empires” have amassed powerful data collections. For example, Solove (2004) reports that there are as many as five data aggregator firms which claim to have data for nearly all of the households in the U.S. He also highlights how firms, such as Wiland Services, maintain databases containing as many as 1000 different data categories for *each* individual in their collection. These data categories include a range of demographics, work and credit history, school records, and consumer behavior. These are comprehensive data bodies. Some of the data empires allow an individual to “opt out,” but they are not necessarily required to do this.[23]

Primarily, digitized data that is rented or sold by aggregators winds up being used by marketers. However, it doesn’t have to be so. If a marketer can purchase or rent the

---

[23] Whether they are required or not is in part a jurisdictional question, as well as a question of where the information originated. The Privacy Rights Clearinghouse provides a list of data vendors who do and do not provide a means for individuals to “opt out” of their database(s) . These are specifically vendors who aggregate *publicly* available data rather than the data that has been purchased from retailers or others who re-sell their customers' information.

data, then what's to stop others from doing so, other than the discretion of the aggregators? Suppose a law enforcement agency wanted to acquire a data set that included personal information. Obtaining the data directly from each individual would require, at the minimum, consent and, absent that, a writ… or possibly not. Again, this depends on the jurisdiction. In the U.S., the government is no less restricted than private firms from *purchasing* data off the market.

As Lyon notes, databases are "leaky containers" (2002a).

It's not just data aggregators, those who specialize in acquiring data for re-sale, who maintain large databases. There are certain industries, such as telecommunications and financial services, where detailed data records of our transactions and relevant "histories" are maintained; moreover, maintaining this data may be required by law and may be a necessity for providing services and billing customers. Also, more complex transactions create more complex data needs and, as in the case with the telecommunications firms, the data is not necessarily complex, per se; we just make a lot of phone calls and these firms provide a vast array of different services. Either way, lots of data is being generated and stored.[24]

The bi-annual WinterCorp survey of government and commercial databases (see Table 2) shows an astounding rate of change. Between 2001 and the 2005 the size of the largest known commercial or government databases increased by 900% and, for the first time ever, exceeded the 100 terabyte (TB) barrier. Another way to assess the magnitude

---

[24]Large databases are not just under the prevue of corporations. The largest known database in the world is at Stanford University. According to their website, as of 2004 the BaBar Database System contained 895 terabytes of data from experiments conducted with Stanford's particle accelerator.

of these databases is to consider the following: The *Yahoo!* database, at 100 terabytes, has the storage capacity to fit enough data for about 2 billion books. That is roughly 120 times the number of books contained in the world's largest collection at the Library of Congress.

Table 2: Winter Corporation's annual survey of database size and performance

2001		2003		2005	
Company/Organization	**Size(TB)**	**Company/Organization**	**Size(TB)**	**Company/Organization**	**Size(TB)**
Telstra	10	France Telecom	29	Yahoo!	100
British Telecom	8	AT&T	26	AT&T[25]	94
United Parcel Service	8	SBC	25	KT IT-Group	49
Experian	3	Anonymous	16	AT&T	27
US Customs Service	3	Amazon.com	13	LGR - Cingular Wireless	25
Korea Telecom (KT ICIS)	2	Kmart	13	Amazon.com	25
Dacom System Tech.	2	Claria Corporation	12	Anonymous	20
CheckFree	1	Health Insurance Review Agency	12	UPSS	19
Centrelink	1	FedEx Services	10	Amazon.com	19
LG TelCom	1	Vodafone D2 GmbH	9	Nielsen Media Research	18

Source: (WinterCorp, 2007) Size in Terabytes [TB]. 1 TB= 1000 gigabytes

This data is acquired in a large variety of ways and on a massive scale and can then be transferred via a network from the collection point where the data was acquired to deposit points in multiple databases. These information flows between different entities around the world are inconsistently managed and regulated. In some jurisdictions, such as the U.S., it is a straightforward task to acquire (through purchase or rent) sufficient information about an individual to potentially cause some real harm. Moreover, the ease of data flows between non-government and government entities varies quite significantly

[25]This is a collection of databases acquired through mergers and acquisitions.

country by country.[26] Varying levels of national regulation aside, however, databasing capacities are growing rapidly and increasingly have a transnational reach.

That all of this data is being collected begs the obvious question: "So what? How could any individual, group, or entity possibly sort through all of the digitized data and makes sense of it?" One potential answer might be found in the market for data analysts. Grossman (2001), however, finds that there is an increasing "data gap" in the U.S., as the demand for new analysts has been flat for over a decade, even as the complexity of the data systems and volume contained therein has dramatically increased.

Given this "data gap," it stands to reason that many valuable insights remain "hidden" in data patterns yet to be recognized and exploited by automated institutional analysis. Only massive computing power can conduct a factor analysis on a matrix that may contain as many as 150,000,000,000 different cells, which is true of the larger data bases.

Data mining

Science has developed a solution to the problem of analyzing massive collections of digitized data: data mining. Data mining has many alternative names[27] and definitions. For our purposes here data mining is defined as;

---

[26] In the EU, for example, data flows regarding personal information of individuals to private industries are currently far more restricted than in the US, though that may change . Whereas in the U.S., despite the "Privacy Act of 1974," there appears a certain "wild west" or (nearly) "anything goes" mentality .

- Non-trivial extraction of implicit, previously unknown, and potentially useful information from data; and
- The exploration & analysis, by automatic or semi-automatic means, of large quantities of data in order to discover meaningful patterns.

Simply stated, data mining is the use of a computer application to comb, sort, assess, analyze, categorize, and explore a vast array of data. Data mining is not merely the "looking up" of a number in a phone book; rather, it's the discovery that the last names Kelley, O'Doules, and McSweeney are more common on the west side of Cleveland along Interstate 90; whereas Spino, LoPresti, and Zingaro are more common on East side (Just west of Interstate 271). At a most basic level, data mining takes raw data (like the phonebook for the greater Cleveland metropolitan area) and turns it into useful insights or, more simply, "information."

In and of itself, data mining represents a great leap forward with respect to taking raw data and turning it into useful intelligence; nonetheless, it has two broad limitations. First, like many operations involving statistical analysis, data mining may be able to indicate corollary patterns and relationships but it is not probative. Secondly, data mining may help uncover the hidden patterns in the data, but it cannot tell the analyst the usefulness or significance of its findings. In other words, data mining detects the latent patterns but it cannot determine what they mean. While the "heavy lifting" of the computations is frequently accomplished with analytical software, the creation or

---

[27]What we refer to as "data mining" has many different purposes, which have resulted in plethora of nuanced monikers, including: knowledge discovery (mining) in databases (KDD), knowledge extraction, data/pattern analysis, data archeology, data dredging, information harvesting, and business intelligence.

selection of the model or algorithm employed and interpreting the outputs is *necessarily* a human function.

Data mining, as a scientific operation, has its modern roots in the late 1980s and early 1990s, and is a synthesis of developments in overlapping and related, but fuzzily distinct, areas including:

- *Statistics*: Theory-based and primarily focused on testing hypotheses;
- *Machine learning*: Focused on improving performance of a learning agent (computer);
- *Knowledge Discovery*: Integrates theory and heuristics to further the process of knowledge discovery, including data cleaning, learning, and integration and visualization of results.

Data mining methods are divided, at the highest level, between two categories. The first category is "prediction," which is a collection of methods that use variables to predict unknown or future values of *other* variables. The most common predictive task is "classification;" however, other classification tasks include traditional regression analysis and deviancy (outlier) detection. Classification is the process whereby a model is inferentially developed from the given data for the purpose of uncovering the previously unknown or hidden relationships. Common uses of classification include direct marketing, fraud detection, and consumer behavior analysis.

The second category is "description." These techniques are meant to find the human-interpretable patterns that describe the data. There are three data mining tasks that are descriptive. First, "clustering" is used to partition data into related subsets. Common

clustering tasks include document clustering or market segmentation. Second, "association rule discovery" is the process of creating dependency rules that can predict an occurrence. A common use of this task is for the positioning of products in a grocery store; for example, stocking novelty cereals at childrens' eye level.

The final task, "sequential pattern discovery," is useful for assessing different variables that have their own timeline of events, in order to find rules that predict the sequential patterns. This is distinctive from the association rule because the association rule is not focused on timing as much as on correlations. An example of this would be the discovery by retailers that people who typically purchase a baseball glove and conditioning oil in February are likely in mid-March to purchase cleats and a batting glove; however, this marketing data may also show that the typical baseball consumer is price-conscious rather than loyal to a certain retailer. With this insight a local sports store might give February customers an incentive to come back in March, such as a 60 day discount coupon for baseball supplies.

These examples seem benign. Most people don't care whether or not the grocery store discovers that children help drive point-of-sale choice. With respect to buying baseball equipment, the "analyzed" customers are probably happy to get something they desire, when they want it, and at a discount. Most people, perhaps after some initial annoyance at being interrupted, are pleased when their bank phones them about simultaneous purchases made with their account in Midtown Manhattan, Little Odessa (Brooklyn), and Moscow (Russia). Your brother-in-law Sergei may have borrowed your debit card but, more likely, you have been victimized by an identity theft ring.

Even benign or benevolent data mining applications can have "unhappy" downsides. For example, cases exist where soldiers returning home from war are put on watch lists because of their recent travels, or babies are prevented from boarding with their parents because their names match adults on the watch lists. That said, much misunderstanding surrounds the risks associated with data mining. Some commentators are quick to point out the power of the technique and assume a negative intent or damaging results. These critics tend to aggrandize the current capabilities of the technology and take its ability to do "something" as a given. Data mining is, in fact, as much art as science and is problem-prone. The problems don't begin with incursions against privacy or civil rights. Fundamental problems with data mining design and operations far exceed those tied to Orwellian metaphors.

Negative spillover effects inherent in mining large data sets are unavoidable. The programmer's aphorism, "garbage in, garbage out" (GIGO), holds that invalid inputs lead to invalid outputs. The phrase is a warning to decision-makers who rely on data analysis technology and assume that what the machine says is right. Technology, moreover, has advanced beyond the literal meaning of GIGO. GIGO implies that invalid results are a direct function of the related invalid inputs. Today's data mining problems may combine dispersed errors that create multiplying effects as they are processed through various networks and stages of analysis. When the errors reside in the network itself, even "clean" data inputs can produce garbage as outputs.[28]

This problem is due to the ability of computers to process even larger "buckets" of data to the point of outstripping their ability to contain negative interactive effects in

---

[28] (Dr. Gary Weiss, personal communication, April 10, 2007).

analyzing the data.[29,30] What follows are biased results from the data mining exercises, which often compounds to create "spillover effects." An error on one level of analysis typically spills over to others, thereby compounding negative effects (i.e., dynamic increase in errors, biased parameters, etc).

A comprehensive assessment of these effects, their potential solutions, and work-arounds has been covered elsewhere with greater detail. However, Yang and Wu's (2005) survey of data mining practitioners provides an parsimonious review of the key problems from the computer scientist's perspective; whereas Seifert and the TAPAC report(s) focus on the public policy and oversight angles (Seifert, 2004; TAPAC, 2004).

DST's and policing

The previous discussion of DST technologies was not specific to law enforcement agencies. The following brief discussion addresses the key DST instruments used in public safety or security, as well as efforts by law enforcement to strategically or programmatically integrate several DSTs (e.g., watch lists) in crime prevention or control.

---

[29] A common problem to many of the effects has to do with algorithms. Algorithms are the set of instructions that dictate the operations of computerized machines. The algorithms make it possible to do the things we do with data: calculate, clean, simplify, sort, store, analyze, and so on. When negative interactive effects arise some of the fixes are insufficient to bridge the gap between naturally occurring errors in the data and the design of the algorithm; moreover, the problems become aggravated as the databases grow

[30] Owners of some large databases have capped or scaled back the growth of the database in order to control this problem .

Police agencies, going back to the invention of the telegraph, camera, and telephone, have endeavored to employ the new and innovative technologies of the day. They adopted these technologies, ideally, to enhance an agency's ability to provide the necessary protections and security desired by citizens; however, we know that this has not always been the case.[31]

As far as surveillance by police in the U.S. is concerned, the checks provided by the Fourth Amendment have been of critical historical importance. However, the Fourth Amendment's reach is being challenged by increasing non-governmental surveillance and police surveillance through DSTs such as CCTVs, which cover increasing swaths of public space[32] where the applicability of the Fourth Amendment is dubious.

Since 9-11 the demand for security, risk reduction, and crime prevention has resulted in the development of a range of strategies related to the pervasive growth and adoption of various DSTs by law enforcement entities. The resulting concerns about law enforcement overreaching and rights violations are not tied to any single DST. It's not necessarily CCTVs or red light cameras or EZ Pass generated travel records. The problem, contend Haggerty and Ericson (1997), is the collected "assemblage" of data and how that data is managed.

---

[31] Examples go as far back as the Civil War and the surveillance of telegraphs. The FBI, under J. Edgar Hoover, was notorious for its clandestine and illegal surveillance tactics against US citizens. That said, illegal use of surveillance technologies and record keeping by law enforcement is not a strictly American phenomenon, see .

[32]For a detailed legal historical review of the permutations of the 4th Amendment and its interpretations in light of technological change, see .

There are a wide variety of DSTs that law enforcement can choose from, but visualization and listening devices are the traditional "bread and butter" categories of surveillance technologies.

Visualization devices, such as closed circuit television (CCTV) cameras have been around for a long time. In fact, CCTV surveillance predated the events of 9/11 by well over 20 years and has been given lengthy treatments by surveillance researchers.

Recent visualization innovations include X-ray devices at airports that penetrate clothing to the skin and thermal sensors that can be used to detect activity in buildings from grow lamps to chemical reactions to the movement of suspects under siege. Listening technologies such as wiretaps, bugs, and parabolic microphones have advanced and miniaturized thanks to digitization; moreover, wireless technologies make it possible to control, undetected, a suspected phone (Georgia Tech Information Security Center, 2008).

Orchestration of DSTs across Law enforcement

More important than any one particular device are programmatic or systematized collections of digitized data by authorities. Frequently, this involves the networking of many devices, which are somehow linked to a data repository. The programs used can facilitate administrative housekeeping to achieve efficiencies or can be aggressively employed for the control or prevention of unwanted behaviors.

On the housekeeping end of the spectrum are systems, such as the one developed by the Belleville Police Department (BPD), which allow law enforcement agencies to digitize and centralize the data that they generate daily from their routine functions. The

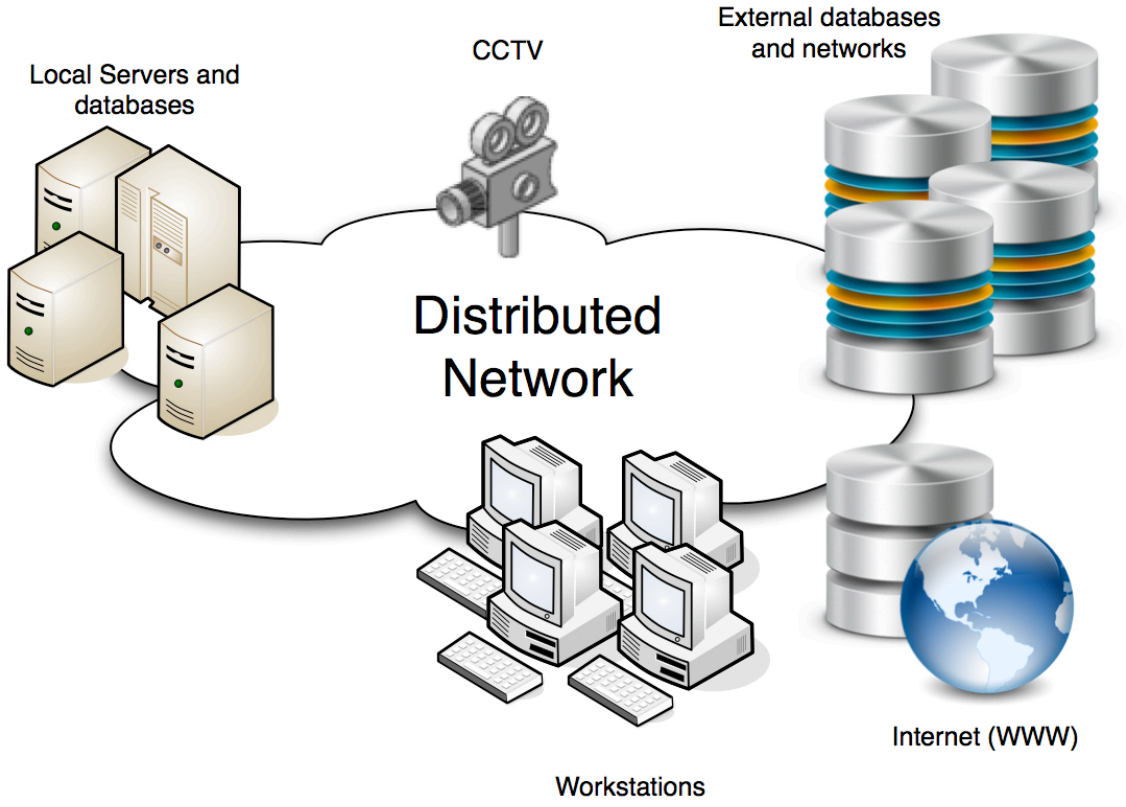
system developed at the BPD and used by over 40 Connchusetts police agencies is called LEAS (Law Enforcement Administration System). LEAS is a networked computerized system that integrates the dispatching, scheduling, and records management functions of the agency. The range of data that the system tracks includes warrants, reports, department equipment, field interviews, training, animal control, shift management, arrests, alarms, booking, and many other functions. There is no doubt that the LEAS system's capacity to quickly collect, organize, sort, and recall information has dramatically increased the efficacy of law enforcement agencies that utilize it.[33]

More advanced DST systems, called "distributed" or "intelligent" systems, involve the simultaneous acquisition and integration of surveillance data from many individual DST devices or disparate systems (see illustration 1). Distributed DSTs have grown in popularity with agencies in large urban areas. For example, since 2001 the NYPD has been incrementally implementing a citywide surveillance strategy, called "Operation Sentinel," that is modeled after London's so-called "Ring of Steel." Among the many DSTs the agency intends on integrating is an interconnected web of 3000 CCTVs in lower Manhattan alone. Once completed, the system will integrate with the surveillance systems from law enforcement agencies within a 50-mile radius of the city. This distributed DST network is intended to maintain a continuous tracking of automobiles into and out of New York City by automatically scanning licenses and searching for suspicious patterns.

---

[33](John DeCarlo, personal communication, August 15, 2008).

Illustration 1: Architecture of a typical distributed DST system



Federal law enforcement agencies, working from the same model as the NYPD, are attempting to develop next-generation CCTV technologies that would involve the distribution of interconnected CCTV systems in hundreds of cities across the county. Developed through the Department of Defense's Defense Advanced Research Projects Agency (DARPA), the program, which was initiated in 2003, was called "Combat Zones That See" (CTS). The objective of the CTS was to create a distributed matrix of cameras and software that would allow police and security agencies to conduct motion pattern analysis across whole cityscapes- including the real-time tracking of cars and people.

Other kinds of DSTs include those developed by the FBI for scanning email, online chats, instant messages, and online phone calls. One program, originally named Carnivore and later renamed more innocuously as DCS 1000, has both trap and trace and full access capabilities. Full access capabilities are much more intrusive than trap and trace methods. Key logging devices can be introduced to a computer as a virus or Trojan horse and, when installed, can record every keystroke that is made. A DST for key logging that is subsumed into Carnivore, Magic Lantern, can be introduced into the computer remotely and without detection by commercial anti-virus software.

The FBI also has a powerful system whereby an agent can perform instant wiretaps of nearly any type of telecommunications device in the US, including cell phones, SMS, VOIP, and land-lines. The Digital Collection System Network (DCSNet), or DCS 3000, provides agents with a simple point-and-click interface where they simply have to type in the phone number of the device in order to access the transmission in real time. DCS 3000 is also integrated into the national network of a private U.S. carrier, Sprint, and can take advantage of the GPS tracking technologies built into the towers.

Mismanagement of DSTs by Law Enforcement

The previous examples of DST devices and/or distributed DST systems are by no means exhaustive. The examples do convey the creativity and expansiveness with which agencies are adopting DSTs. What is of primary concern in this research is to understand how DSTs are chosen, designed, implemented, used, maintained, and interconnected so that the systems, and the data they contain, can be controlled or prevented from

facilitating the abuse of citizens' rights. In a society where our relations are increasingly mediated by technologies that permit widespread surveillance, the incentives for law enforcement to acquire, collect, and mine data are powerful drivers of information policy. The potential for ineffective controls and negative impacts are not insignificant issues for any police agency adopting or expanding DST technology.

Nonetheless, how well local law enforcement agencies manage their DSTs is largely unknown. To date, there have not been any empirical studies assessing DST management by local police. However, the documented DST problems of the U.S.'s elite law enforcement agency, the FBI, and recent reports and Supreme Court cases clearly show that local and state level police agencies are not immune to serious and, in the words of Justice Ruth Bader Ginsburg, "systemic errors" with DSTs employed by law enforcement ("Arizona v. Evans," 1995; Auditor Of The Commonwealth, 2009; Herring v. United States," 2009). These cases strongly suggest there is cause for deep concern about how police agencies are managing such systems

The need for this kind of direction to practitioners and policy makers at the state and local levels is underscored by recent events such as the newly (May 5, 2009) released audit of police abuses of data systems in Massachusetts (Auditor Of The Commonwealth, 2009). This report showed a pervasive pattern of abuses by law enforcement in using the systems expansive data collection for unauthorized inquiries; however, as the report identifies, the procedures and technologies to track and or delimit uses of the statewide databases are not present. As such, anyone, once inside the system can view, alter, or destroy the data in the system with impunity. In responding to the release of the report

some experts argued that this is a pervasive problem in many jurisdictions and in other fields, especially health care (Moscaritolo, 2009).

Few law enforcement agencies have the breadth and depth of personnel and array of responsibilities of the FBI. With respect to DSTs, the FBI has been an "early adopter" and innovator. However, the agency's record of successfully designing and implementing data management and acquisition systems that meet the stated objectives and are properly controlled is poor. For example, a 2002 study commissioned by the US Attorney General found:

> …significant deficiencies in Bureau policy and practice with respect to securing data held by the agency… Those deficiencies flow from a pervasive inattention to security, which has been at best a low priority. In the Bureau, security is often viewed as an impediment to operations, and security responsibilities are seen as an impediment to career advancement.

Since 2002 it would appear that much has changed about the FBI's mission and the way the Bureau attempts to publicly portray itself as an intelligence-oriented police agency but, in fact, little has changed about the culture. According to Shane and Bergman, the

> … F.B.I. culture still respects door-kicking investigators more than deskbound analysts.… The uneasy transition into a spy organization has prompted criticism from those who believe that the bureau cannot competently gather domestic intelligence, and others, including some insiders, who fear that it can.

In a statement to Congress, the Department of Justice's (DOJ) Inspector General cited the “significant challenges and deficiencies” which persist at the Bureau - in part due to entrenched cultural and bureaucratic norms. In that same testimony, the Inspector General went on to criticize the Bureau in a number of critical areas, especially with respect to oversight:

> The FBI needs **more improvement** in critical areas such as upgrading its IT systems; balancing aggressive pursuit of its law enforcement and intelligence-gathering missions while **safeguarding civil rights**; hiring, training, and retaining skilled employees in a variety of critical occupations; sharing information effectively within and outside the FBI; **monitoring** its allocation of **resources** between its law enforcement and intelligence functions; maintaining **vigorous internal security** and counterespionage efforts; and ensuring the reliability of its scientific methods. These are not easy tasks, and they **require constant attention and oversight**… the OIG will continue to attempt to conduct **vigorous oversight** of FBI programs [Author’s emphasis].

Entrenched bureaucratic and procedural norms of the FBI support a “do what you have to do, but don’t get caught” mindset. This message, and the Bureau’s history of lax controls, invites unwanted behaviors. A review of internal FBI documents pertaining to the DCS 3000 program procured through a FOIA request by the Electronic Frontier Foundation found that the existing internal controls against system abuses or theft of data

by rogue agents or spies presented a "grave threat." One example of "…widespread and serious misuse" of data by the FBI was documented in a report by the DOJ Inspector General regarding the controversy over cell phone record data obtained from phone providers by the FBI vis-à-vis the FISA court. Another pertains to the documented loss of laptops owned by the agency: a 2002 audit found a startling number of laptops had gone missing in a 2 year period. To make matters worse, there was no procedure or formal documentation associated with the thefts and no way to confirm whether or not sensitive data had been compromised. Follow-up audits found a reduction in per-month thefts of laptops; however, procedures for documenting the precise loss of data were still found to be wanting.

There have been many questions regarding the legality and oversight mechanisms pertaining to the collection or sharing of information on individual citizens by the FBI. In 2005 the Bureau was compelled by the courts to release documents pertaining to civilian surveillance activities authorized by the U.S. PATRIOT Act. The internal documents provide direct evidence of information illegally obtained, with limited supporting documentation, and lack of supervision by administrators over the activities of employees. The agency argued that data that was illegally obtained was "quarantined and eventually destroyed." However, given the lack of controls, there is no assurance that all copies of the data were purged or that the information hadn't been used in investigations. The concern about lack of controls regarding data acquisition and maintenance is exacerbated by discoveries of both cover-ups and public FBI acknowledgements, in Congressional hearings, of serious weaknesses in the oversight of these systems.

So far the discussion has centered on the use (and abuse) of in-place DST systems. What about oversight as it pertains to the selection, design, creation, implementation of new systems? Increasingly, this involves contracting with outside vendors, which means that a police agency is going to have to manage third parties. In the case of the FBI, a lack of internal capacity to run a software project led to the $170 million boondoggle known as the "Virtual Case File" (VCF). The VCF was meant to be a significant upgrade to the record management system used by the Bureau;[34] however, the project was cancelled in 2004, one month before it was supposed to be completed and after almost three years of development. Simply put, the Bureau had agents "tasked" to the managment of the project who had no substantive expertise, other than that they were sufficiently ranked to "manage outsiders" working for the Bureau.

Summary of Mismanagement of DSTs by the FBI and its connection to the proposed research

What the issues and cases raised in the preceding pages plainly show is that that the U.S.'s most elite police agency, the FBI, has ongoing and serious problems with respect to the oversight and control of DSTs. That the problems exist and persist is a matter of public record. Also a matter of public record is that no single cause, whether cultural, structural, or criminal, can neatly explain each of the incidences described. In other words, the cause or causes vary based on the specific DST and the context.

---

[34]In many respects the VCF system was the FBI's equivalent of LEAS, see above.

The recent history and experiences with DSTs that the FBI has had gives direction to the proposed research. Though there are dramatic differences in scale and scope of DSTs between the FBI and the local police (who will be the object of this study), functional and cultural parallels between police agencies at all governmental levels and across jurisdictions suggest that what the FBI encountered is a harbinger for law enforcement agencies generally. Moreover, the DST issues addressed in the review arise in smaller scale applications, and even local police agencies operate nodes in the same networked surveillance systems as their state and federal brethren.

The potential for abuses and misappropriations of the powers delegated to law enforcement agencies and their employees is real, but it is not a given. In other words, law enforcement agencies' use of DSTs does not necessarily lead to social harms and undesired outcomes. That said, police play a special role in society and are thus given unusual powers to fulfill their dual “care” and “coercion” role. Surveillance is inherent to this mission, and the use of DSTs is but an extension, but the pervasive reach of these technologies into our lives make it imperative that we understand as fully as possible how these systems work in everyday policing.

Toward effective oversight of DST regimes: Entrée to Situational Crime Prevention

The DSTs can be quite advanced and law enforcement agencies, at the highest level, have had difficulties in adjusting existing means and methods of oversight. While the FBI has been a frequent target for derision, insufficient oversight and accountability of DSTs has created many opportunities for a wide variety of negative externalities by law enforcement agencies or their employees, both in the U.S. and abroad. Clearly,

oversight and accountability has not kept pace with the rate of change caused by the adoption of DSTs. Current regimes of oversight are *post-facto,* poorly-planned, fragmented and, in some cases, border on non-existent.

The wide variety of particular DSTs and the extraordinary variety of contexts that they can be employed in renders the specter of a convenient "one-size fits all" solution to oversight an idealized and unrealistic fairy tale.

What is needed is a protocol for practitioners and overseers of DSTs to help facilitate the design of contextual and situationally sensitive preventive or control mechanisms. A way forward that is designed to fit the reality of the networked environments in which DSTs operate and that makes it possible for expressly delimit and deter harms rather than react to their occurrences is necessary.

If we take harms to mean "unwanted behaviors that result in undesired consequences," then it is reasonable to look to existing literature that focuses on the reduction and prevention of crime. After all, a crime is a particular type of an unwanted behavior that has been legislated as such, due to the undesired consequences of its commission. Two streams of literature that could illuminate abuse prevention with respect to DSTs are Situational Crime Prevention (SCP) and Information Systems (IS) security. Each is discussed below.

Situational Crime Prevention

SCP is an elaboration of a much larger framework called "Crime Prevention Through Environmental Design" (CPTED). CPTED, and by extension Situational Crime Prevention, draws upon a diverse set of ideas to articulate a framework for preventing the

commission of unwanted behaviors.[35] Central to CPTED's theme is that *crimes are a function of opportunities present in the physical environment*. This is not a causal relationship but a necessary one. Thus, if we can understand the opportunity structure of crimes themselves and the environments in which crimes take place, then we have a greater likelihood of preventing crimes. As simple as this idea appears, it is not without controversy or critics.

Situational Crime Prevention subsumes earlier CPTED frameworks.[36] Unlike previous CPTED elaborations, SCP is not exclusively focused on predatory offenses and

---

[35]Articulating even a simple run-through of how CPTED developed can be confusing. This is due to the fact that the term is both the name of a theory and one of its elaborations. Key to the historical development of CPTED is its conceptual roots from innovations of urban theory developed in the 1960s: social control through natural surveillance , environment and crime , and environmental opportunities and offender choices. Arguably, CPTED follows an integration model incorporating ideas from a variety of sciences including psychology, economics, and physiology.

[36]The term Crime Prevention Through Environmental Design was first coined in 1971 by C. Ray Jeffery. His main argument was that positivists had overplayed the impact of sociological factors that lead to crime and had understated the environmental and biological connections. Jeffery's level of analysis was largely micro and sub-micro. Jeffery believed that in order to prevent crime we had to look at the "total environment," which meant assessing the connections between the offender's immediate environment and his/her psychological and physiological factors. "Defensible Space" (O. Newman, 1972) was published around the same time as Jeffery (1971) and was based on many of the same ideas. However, Newman's analysis was decidedly macro. He argued that most crimes occur in public housing because they were large, had fortress-like aesthetics, and "designed out" a sense of community or privacy. This resulted in an increase in the fear of crime and discouraged people from taking responsibility in their neighborhood, thereby lessening the natural surveillance. Crowe , a disciple of Jeffery, took CPTED to the "next generation" by integrating Newman's and Jeffery's ideas and responding to early criticisms. Both Newman and Jeffery were criticized by mainstream

fixed environments. SCP is oriented toward "situational" analysis of behaviors and the environments in which they occur. It does not look at all crimes as being generically the same, and therefore does not advocate a one size fits all solution. Nonetheless, SCP is a generalized approach to crime prevention designed for use in any environment with any manner of crime. The key difference is that the methods of SCP can be used to assess a specific situation and crime problem to customize a solution:

> Situational prevention comprises opportunity-reducing measures that (1) are directed at highly specific forms of crime, (2) involve the management, design or manipulation of the immediate environment in as systematic and permanent way as possible, (3) make crime more difficult and risky, or less rewarding and excusable as judged by a wide range of offender. (Clarke, 1997)

SCP was initially derived from practical and theoretical advancements made in the late 1970s by Clarke, Cohen, Felson, Goldstein, and Mayhew (Clarke, 1980; Clarke & Mayhew, 1980; L. Cohen & Felson, 1979; Eck & Spelman, 1987; H Goldstein, 1979; Mayhew, Clarke, Hough, & Sturman, 1976). SCP has been combined with an "action research" approach to problem solving which has been "codified" by the U.S. Department of Justice into the SARA method. With SARA, practitioners are encouraged to work in a collaborative and iterative fashion until a satisfactory understanding and solution to the crime problem is found.

---

criminologists as being "simplistic," relating humans to animal behavior, and guilty of "environmental determinism;" also, Newman's work included statistical errors, which only made him an easier target.

SCP employs a series of analytical tools and methods for diagnosing specific crime problems and prescribing and implementing tailored solutions. These tools make it possible to make macro, meso, and micro level assessments of crime problems. Creating and implementing solutions using SARA, practitioners employ a combination of operationalized "techniques" (see illustration 2, below) that can be incorporated in part, or in whole, to tackle a specific problem.[37]

The tools of SCP have been refined and honed over several years, however, SCP case studies and interventions have been focused in one of three ways:

Environment-oriented

The SCP protocols have been implemented in colleges, bars, amusement parks, drug markets, and bus terminals to comprehensively modify these environments to reduce unwanted behaviors.

SCP Technique-oriented

These cases applied one of the 5 broad SCP technique categories (see column headings in illustration 2) or applied some specific combination from the techniques.

Crime-oriented

These cases have applied SCP techniques to deter specific crimes such as robberies of convenience stores, car theft, and the sexual abuse of children.

---

[37]The current list of twenty-five "techniques," is the latest iteration as the total number of techniques has evolved and expanded since initial introduction. These evolutions are a direct function of both theoretical and empirical advancements in SCP.

Illustration 2: Twenty-five techniques of SCP

Increase the Effort	Increase the Risks	Reduce the Rewards	Reduce Provocations	Remove Excuses
1. Target harden ▪ Steering column locks and immobilisers ▪ Anti-robbery screens ▪ Tamper-proof packaging	6. Extend guardianship ▪ *T*ake routine precautions: go out in group at night, leave signs of occupancy, carry phone ▪ "Cocoon" neighborhood watch	11. Conceal targets ▪ Off-street parking ▪ Gender-neutral phone directories ▪ Unmarked bullion trucks	16. Reduce frustrations and stress ▪ Efficient queues and polite service ▪ Expanded seating ▪ Soothing music/muted lights	21. Set rules ▪ Rental agreements ▪ Harassment codes ▪ Hotel registration
2. Control access to facilities ▪ Entry phones ▪ Electronic card access ▪ Baggage screening	7. Assist natural surveillance ▪ Improved street lighting ▪ Defensible space design ▪ Support whistleblowers	12. Remove targets ▪ Removable car radio ▪ Women's refuges ▪ Pre-paid cards for pay phones	17. Avoid disputes ▪ Separate enclosures for rival soccer fans ▪ Reduce crowding in pubs ▪ Fixed cab fares	22. Post instructions ▪ "No Parking" ▪ "Private Property" ▪ "Extinguish camp fires"
3. Screen exits • Ticket needed for exit ▪ Export documents ▪ Electronic merchandise tags	8. Reduce anonymity ▪ Taxi driver IDs ▪ "How's my driving?" decals ▪ School uniforms	13. Identify property ▪ Property marking ▪ Vehicle licensing and parts marking ▪ Cattle branding	18. Reduce emotional arousal ▪ Controls on violent pornography ▪ Enforce good behavior on soccer field ▪ Prohibit racial slurs	23. Alert conscience ▪ Roadside speed display boards ▪ Signatures for customs declarations ▪ "Shoplifting is stealing"
4. Deflect offenders ▪ Street closures ▪ Separate bathrooms for women ▪ Disperse pubs	9. Utilize place managers ▪ CCTV for double-deck buses ▪ Two clerks for convenience stores ▪ Reward vigilance	14. Disrupt markets ▪ Monitor pawn shops ▪ Controls on classified ads. ▪ License street vendors	19. Neutralize peer pressure ▪ "Idiots drink and drive" ▪ "It's OK to say No" ▪ Disperse troublemakers at school	24. Assist compliance ▪ Easy library checkout ▪ Public lavatories ▪ Litter bins
5. Control tools/ weapons ▪ "Smart" guns ▪ Disabling stolen cell phones ▪ Restrict spray paint sales to juveniles	10. Strengthen formal surveillance ▪ Red light cameras ▪ Burglar alarms ▪ Security guards	15. Deny benefits ▪ Ink merchandise tags ▪ Graffiti cleaning ▪ Speed humps	20. Discourage imitation ▪ Rapid repair of vandalism ▪ V-chips in TVs ▪ Censor details of modus operandi	25. Control drugs and alcohol ▪ Breathalyzers in pubs ▪ Server intervention ▪ Alcohol-free events

Source: (R. Clarke & J. Eck, 2006)

Leading SCP theorists have argued that the SCP framework can apply to technologies and oversight mechanisms.[38] That said, the literature from criminologists as it might pertain to DSTs tends to focus on exogenous threats, including terrorism, hacking, fraud, and identity theft (G. R. Newman & Clarke, 2003).

There is yet to be, from criminologists, a way forward for SCP to provide a framework for the control or prevention of endogenous threats as they relate to DSTs; however, emerging ideas from the information security literature provides a head-start, and these are described below.

---

[38] Although Eck's (2008) argument regarding oversight is *not* limited to technology-laden environments.

Information Security and SCP

Information security (IS) practitioners are responsible for protecting the full range of information technologies that organizations employ from the panoply of attacks frequently launched against these systems. As Willison (2008) illustrates, existing IS literature is atheoretical and focused on technical-oriented safeguards and deterrents to unwanted uses of information systems; moreover, Willison convincingly argues that SCP and traditional IS analysis have much to offer each other in the context of addressing the "insider" threat.

Willison (2008) examines the 25 techniques of SCP (see above) and advances his own elaboration based on existing IS security controls. For example, he states that one means of "target hardening" is to apply "physical locks for PCs" in order to enforce the physical security of computers. Another example is to "reduce anonymity" by having visitors wear ID tags. These ideas are useful and applicable to the proposed research, but they are not sufficient. With DSTs, the physical environment is only a part of the space to be protected and defended; moreover what Willison does not address is how to secure and delimit errors associated with the normal uses of the system and the data contained therein.

With DSTs there are issues of design and oversight of the software and the networks on which the data flow. Willison appreciates the software/network problem, and proposes a further integration of IS and SCP. Specifically, he adopts an earlier idea from Cornish by calling for the creation of "crime scripts" specifically tailored for the IS practitioners. "Crime scripts" are context sensitive, sequential narratives of the steps

needed to commit the unwanted behavior. By modeling the necessary steps it is possible to identify the specific combination of SCP techniques that would have the greatest efficacy given the context in which the interdiction is to be implemented.

Conclusion

The social science literature concerning the controlling or preventing unwanted behaviors and consequences of DST's plays out long-standing theoretical debates, features dire warnings extrapolated from single case failures, and only recently (Willison, 2008) has proposed holistic approaches marrying preventative concepts such as SCP with a working command of how DSTs actually operate. However, law enforcement agencies now have access to powerful DSTs that have been shown, at all levels of government, to lack clear and reliable protocols to protect against abuses of privacy, citizen rights, and governmental oversight. And since no researcher has so far comprehensively studied the full scope of DSTs in operation in a police agency the veneer in which these abuses take place remains a "black box"

Thus, this project endeavored to extend this literature with an embedded case study situated at the center of an operational DST system operated by a police agency.

Chapter 3: Research Design and Methods

Sample, Single Case-Study

Most police agencies are extremely reluctant to provide researchers with the access necessary to fully comprehend DSTs in action, particularly if understanding misuse and abuses is part of the inquiry. In developing this project several federal and state agencies were approached and it became clear to the researcher that obtaining access was going to be a major hurdle. The ideal situation would have involved an embedded researcher who could access and simultaneously study the necessary technologies, actors, and documentation to the extent that is permitted by law.

After several agencies demurred, the Belleville Police Department (BPD)emerged as a highly promising study site. The BPD's executive officers were enthusiastic about providing the researcher the necessary access; also, the agency itself has a combination of characteristics that makes it representative of police generally but also distinctive for its advanced DST system:

- In 1999, BPD was the first agency to implement a third-party software system, the Law Enforcement Administration System (LEAS), which was designed to integrate all the key areas of routine and critical police, fire, and EMS functioning into a common digital surveillance system. This includes the spectrum of functions including dispatch, prisoner booking, evidence management, and case reports, which are all integrated into a single data management system.

- The current Chief of the BPD, Bernard Sowley, was also the lead software designer on that system. Since 1999, LEAS has been adopted by over 40 Connchusetts agencies including, most recently, the State Police.
- In 2006, BPD contracted with a Canadian technology provider to create a data mining tool that would allow them to conduct pattern analysis of case reports that are generated and maintained in their jurisdiction.
- Additionally, the BPD contracts with a web-based U.S. data collection service that allows investigators to conduct thorough background checks on citizens. This private and fee-based service available to police agencies aggregates information that, if separately obtained from the data originator, might require the issuance of a warrant.
- The BPD is currently implementing an installation of mobile CCTV posts.
- In addition to their own data collections and outside vendors' data collections, the BPD uses a selection of federal and state DSTs that are available to all police agencies in its state.[39]

In June of 2008 the researcher provided the executive officers of the BPD with a draft proposal to analyze their data systems. Serendipitously, the BPD was at that time considering hiring a third-party consultant or partnering with a qualified academic to

---

[39] Some of these are data collections that employees can access and, in some cases, the BPD can both contribute to and collect data from them.

assess and audit their data systems.[40] They had added so many features, functions, and new applications since 2001 that no one had a complete view of all of their data collection, surveillance, and management technologies. The BPD invited the researcher to collaborate with their employees and to facilitate an assessment of their complete system with the agreement that the researcher would, in turn, be able to use the findings for the purposes of this research.

The researcher thus was given entrée to do what he had done in his previous career as a technology consultant- to perform an in-depth analysis of the BPD's DSTs and systems from a business perspective. In social science terms, the researcher was invited by the agency head to evaluate or otherwise closely examine the public benefit of the agency's program(s) and to explore possible needs, changes, or alternatives. This research would thus involve a combination of ethnographic and embedded case study methods.

While this researcher's overarching design for this embedded case study presumed a mainly collaborative relationship with agency executives and employees, it was anticipated that, at particular times and for particular operations, the researcher would be approaching certain employees more like research subjects. Accordingly, the John Jay Institutional Review Board considered the applicability of human subject protections in the proposed research. A waiver was granted upon the determination that this research was taking place entirely within the realm of a public organization, upon the

---

[40] According to BPD Chief DeCarlo, their preferred approach in other areas has been to partner and collaborate with academics. The BPD has a long-standing relationship with University of Old Gotham (UNH). UNH crime prevention researchers conduct weekly COMPSTAT meetings with the BPD.

invitation and authority of the agency executive, where any employees observed or interviewed would be engaged in official duties subject to such authorized review, whether by auditors, consultants or, as was the case here, an invited researcher.

Overview of Ethnographic and Embedded Case study methods

Ethnography and embedded case studies have unique advantages when exploring emergent phenomena and in studying populations and social environments, such as organizational operations within police agencies, that are hidden from casual observation (Lambert, 1990; Lee, 1995; Marx, 1988; Trotter, 1999; Weppner, 1977). This type of study requires extended work in the naturalistic settings in which the investigated activities take place. Using field notes, logs, transcribed interviews, and other textual sources, ethnographers systematically develop more comprehensive descriptions of social worlds and their participants. To check the veracity of the data gained through fieldwork, extensive follow-up with collaborators is essential. Establishing trust with collaborators often requires a lengthy period of time, especially when talking to police employees about how their DSTs and systems and operations function out of view of civilians.

While the true subject of this study is, in fact, the non-human DSTs, the researcher is dependent on the police in Belleville, the "everyday users," to be collaborators. Given the sensitive nature of this topic, individual officers or employees may have initially been wary of the motives of the researcher. While the researcher is experienced in overcoming these difficulties in other venues, it is always a process that requires time and effort.

This combined methodology is uniquely capable of addressing the complex

dynamics of working with police behind the scenes(where they are not normally scrutinized by citizens), and permits the development and constant refinement of hypotheses and theories based on multiple sources of data and modes of analysis (Brewer, 2000; Creswell, 2007; Denzin & Lincoln, 2008; Scholz & Tietje, 2002; Werner, Schoepfle, & Ahern, 1987).

The research design allowed for the building-in of cross-checks of information and enabled the researcher to synthesize multiple viewpoints, heavily contextualizing each phenomenon to facilitate arrival at a holistic and multifaceted rendering of reality (Bernard, 2006).

A study such as this required knowledge integration related to different disciplines, systems, and interests. Moreover, throughout the case study multiple sources of evidence and data were obtained in order to achieve the fullest and most accurate picture of the issues under study. The methods employed are discussed below. Because this project was conducted in a non-linear and iterative fashion, the order of discussion does not reflect the order in which the methods were applied. Methods were applied as circumstances dictated and had a cumulative and increasingly synergistic impact over the course of the study. It is worth briefly noting here, however, the extent to which various methods were employed.

This researcher conducted over 120 interviews, divided about equally between agency and Town executives, command officers, and line employees. More than 400 hours over a period of nine months was spent observing employees during the course of their work. This researcher spent many more hours reviewing hundreds of reports, memos, coding sheets and contracts housed in archival agency records. The analysis of

content and data, the distillation of key concepts and events, the synthesis, testing and refinement of emerging conclusions—in short the formal writing of this dissertation—fully occupied this researcher for nearly four months.

Direct observation

Direct observation plays several crucial roles in the research process and it is the principal strength of ethnography, in that it enables the researchers to triangulate data obtained from multiple sources of data collection, thereby using their privileged position to assess the accuracy and truthfulness of what they hear and see (Adler & Adler, 2000; Atkinson & Hammersley, 2000; Spradley, 1979). Direct observation educates the researcher about the differing contexts in which different specific systems and applications are used by the BPD, how those different systems are used differently by the various users of the system(s), in what ways the system(s) prevent or enable users to do their jobs, and how the systems impact and are impacted by the organization of the police and their routine and critical functions. It also allows the researcher to make connections and construct hypotheses that may remain invisible to or obscured from subjects, and makes it possible for the researcher to witness new developments as they occur.

In this study, the researcher directly observed employees of the BPD who were using digital surveillance systems in their natural settings, such as the telecommunications center, patrol cars, booking and evidence rooms, and the Detective Bureau. The most extensive observations took place in the telecommunications center, where this researcher was present for the equivalent of five tours of duty, spread among day, evening and overnight shifts. The research also was brought along on 10 police

cruiser runs to observe officers, and their equipment, in action. All of this allowed the researcher to observe the full range of uses of the data system(s) such as documenting and retrieving reports, dispatching and directing calls for service, booking suspects, investigating cases, managing cases, sharing of data with exogenous law enforcement systems, and the maintenance of the systems.

Interviews

Interviews, as a general rule, help the researcher learn about how collaborators perceive their social worlds(Fontana & Frey, 2000; Gorden, 1980; Merton & Kendal, 1946; Patton, 2002; Survey Research Center, 1976). In this study, the principle object of this study is a series of stand-alone and networked computer systems that enable the BPD to conduct regular digital surveillance. However, the employees/collaborators at the BPD were interviewed in order better understand the systems under use, how they are used, how the BPD integrates DSTs developed in-house with the state or federal systems. This research went beyond everyday practices and sought to understand the manner in which the BPD chose, adopted, designed, implemented, and tested these systems in the past. Initially, open-ended interviews were employed; however, these interviews and interactions were guided by research questions presented in chapter one. These interviews provided the researcher the opportunity to build rapport with his collaborators, as well as gain an understanding of how the systems work. Interviews were conducted with a range of necessary personnel, such as 911 operators, police officers, detectives, case transcribers, executive officers, and IT Staff. Many of the employees play different user roles in the different systems employed by the BPD. In other words, a police officer and a

detective may both have access to a particular DST but each may have different limitations put on how and when and for what purpose they access the DST. Given this reality, these guided open-ended interviews permitted an adaptable format that can vary with the interviewees' job and user role within the system. The open-ended interviews allowed the researcher to gauge important themes such as the extent of the use of DSTs systems, the effects of DSTs on the organizational structure of the BPD, and the efficacy of the DSTs. The interviews also allowed the researcher to develop an inventory of the state and federal systems available to the local police, investigate the roles and processes in the creation or adopting of new surveillance technologies, and discover how the system(s) delimit harms. In these discussions, the researcher introduced various themes, while allowing the participants the freedom to discuss them in their own manner and words. In this way, interviewees were able to introduce unanticipated topics many of which were of great importance.

The directed open-ended interviews, coupled with the direct observations and the secondary data analysis described below proved an efficient way of getting a view of the "big picture," and lead to more direct inquiry. As information and insight was assembled, it led to the need to acquire specific information to clarify or prove/disprove a particular issue; thus, over time, it was necessary to conduct focused follow-up discussions with various individuals.

Archival Records and Content Analysis

Archival records, in general, provide an important opportunity for data collection. Content analysis provides the researcher with a systematic means for analyzing data

obtained from public and private archival sources (Denzin, 1989; Krippendorf, 2004; Neuendorf, 2002; Shaw & Gould, 2001; Singleton & Straits, 2005). This provides the researcher with the ability to not only observe people's current actions and words but also to "observe" the historical decision-making that resulted in the present context (Frankfort-Nachmias & Nachmias, 2008). When assessing a complex technical environment, archival records become a necessary tool for auditing the design, construction, and implementation of individual sub-systems, as well as issues pertinent to the entire system. For this research it was important to obtain and analyze an array of documents, including the architectural and design plans for the software and its integration, user manuals, roll-out plans, internal memos, and quality assurance (QA) documentation. Fortunately, the majority of these documents, going back to the 1970s had been maintained by the BPD in an organized way, and the researcher was given complete access to the appropriate files and records.

Data Analysis and Synthesis

By the end of the research, the researcher reviewed, assembled, or created:

- Ethnographic data from 9 months of fieldwork;
- An understanding of applications and functions of all of the digital surveillance acquisition, sharing, or management systems;
- An understanding of the user roles and their usage patterns of the systems;
- Flow charts identifying the way that data is passed-off and made accessible between the user groups and systems;

- Flow charts illustrating how information is locally generated and by whom, and how it is managed and made accessible at various stages –both within the agency and exogenously;
- Images of how the various applications appear to the user (screen shots);
- A detailed break-down of the features of all of the BPD surveillance applications and their roles in supporting the routine and critical functions of the BPD.

The mechanics and strategies for analyzing this data deserve some discussion.

Because the BPD invited the researcher to collaborate with its employees in conducting this research, the agency provided useful resources. For example, the researcher provided office space with a locked file cabinet, phone, etc. Also, the Deputy Chief (who also worked directly with the Chief in building LEAS, and has daily oversight of the running of that system) worked directly with researcher to facilitate the researcher's resource needs (helping to set up interviews, etc.). The data collection, management, and analysis of the data was centralized at the BPD offices in Belleville. That said, there were strict guidelines established by the BPD that prevented any documents or memos from being removed from the premises of the BPD headquarters. The exceptions were agency approved photographs of their facilities and screen shots of their DSTs.

Analysis of the data necessarily involved the use of techniques that are not normally found in the "toolbox" of social scientists. Simply put, much of the data was technological in nature and the researcher had to conjoin an understanding of police

operations with his knowledge of the SCP framework and his expertise of the design and construction of data surveillance systems.

The SCP framework for case study evaluations is exceptionally well suited for analyzing traditional crime problems, using the framework to design a response to the problem and assess the efficacy of the response. It was originally posited that the tools of SCP have not been sufficiently modeled to assess and develop an interdiction and analysis protocol as is proposed here. However, recent literature has emerged that synthesizes new protocols using the SCP framework to control prisons (Wortley, 2002), and to prevent cyber-crime and terrorism (Clarke & Newman, 2006; G. R. Newman & Clarke, 2003). This present study built from Willison's (2008) showing a conceptual connection between SCP and the digital environment.

Stake (1995) contends that aggregating data into coherent categories for analysis is one way of approaching the analysis of data. To that end, evidence and information uncovered by the researcher was categorized with respect to their relevance to the research questions through the use of color-coded sticky (Post-it) notes arrayed on boards. The boards were added to and modified daily and helped sort and analyze the vast collection of information that was assembled during this research. Also, as Yin (2009) notes the analysis is furthered by assembling a quantum of relevant evidence focused on the purpose of the study. The researcher's prior, expert knowledge in the field of DST design and assessment also contributed to and furthered the analysis

The following chapters present, in order, a review of the setting, the 30-year development of surveillance technologies in Belleville, and a detailed accounting of the current status of the organization, use, and oversight of these technologies by law

enforcement in Belleville. These chapters are the result of an amalgamation of information and insights gained by using the aforementioned data collection methods. To maintain anonymity of the town, the state, and the individuals it was necessary to use 'anonomizing' techniques, such as pseudonyms and obscuring of individual's identities in photographs and screen shots.

Hypothesis Formation, Testing and Refinement

Explanations of the relationships between users, user roles, systems and applications, accountability and oversight, and the routine and critical uses of the systems evolved toward hypotheses as data accumulated that supported them.

As the field observation period progressed, the researcher reviewed and sorted through the data and documents carefully to understand how best to assess the research questions and build them into broader schemes, themes, and hypotheses. Hypothesis testing took place as fieldwork continued with the expressed purpose of seeking probative and negative cases that supported and challenged the initial hypotheses. As the fieldwork proceeded, this process continued in a "feedback loop" of "constant comparative analysis" (Glaser & Strauss, 1968).

After using this layered, iterative process to portray what was occurring (description),the researcher worked on explaining why the phenomena occurred as they did (analysis). The final stage (synthesis) was to propose a set of data collection protocols, aligned with existing protocols of SCP, which can be used to:

- Assess the oversight and accountability risks in *existing* systems; and

- Design *new* systems, where accountability and oversight risks are mitigated from inception through implementation.

Apparent paradoxes, contradictions, and complex relationships revealed by the findings were particularly useful in illuminating unarticulated assumptions that challenge the hypotheses and also suggested pursuing avenues for future investigation. In the final months of the project, further analysis of the data took take place by subjecting the data collected through fieldwork to the process of data reduction.

Data reduction proceeds by organizing field notes, interview data, concept papers, technical notes, and theory notes into computer files that reflect the dominant themes that have emerged through the research process. This study drew on ethnographic research in the presentation of narratives, vignettes and case studies that reflected the dynamics and complexity of the findings; however, since the technical side of the socio-technical system is a major study focus, descriptive charts, matrices, and flowcharts were also developed as needed (Creswell, 2007; Patton, 2002).

Biographies of subjects directly mentioned by name in this study

This study was approved as having an "exempt" status by the John Jay College of Criminal Justice IRB. This was due to the fact that the thing under study was the surveillance technologies and all of the people involved were involved as part of their public duty as employees of a law enforcement agency and that the manager for that agency had invited the researcher into the agency. That said, during the proposal stage it was recommended that any reference to individuals, the agency, or the state be anonomized. This was meant to protect individual identities in case the researcher

uncovered potentially damaging information. While many individuals were interviewed, formally or otherwise, only a few are explicitly named and quoted. Those who are are listed below with a brief statement about who they are:

- *Chief Bernard Sowley*. Sowley is the current Chief of the Belleville Police Department. He has over thirty years experience in law enforcement- which includes a 2 year stint with the FBI. He holds an undergraduate degree in computer science and spearheaded the major initiatives to develop the range of surveillance technologies employed by his agency, going back to the late 1970s.
- *John Arendosh*. Was a part-time police officer in Belleville and a computer programmer for a financial services firm in a nearby town. Along with Bernard, he built the DSTs in Belleville and, in the mid-nineties retired to start his own software firm that licenses the digital record management software that he and Bernard originally built for the Belleville Police.
- *Lieutenant Dan*. Is an 18-year veteran of the Belleville Police. He has an undergraduate degree in computer science and worked as an IT professional before he switched careers in 1990. He is the chief administrator for the Belleville information systems.
- *Lieutenant Picasso*. Is a 15-year veteran of the Belleville Police. He is a "cop's cop"- doggedly relentless and by the book. During this research he investigated and solved a string of major bank robbery cases that required a

sharing of DST resources between various local municipalities and federal agencies.

- *Detective Travis*. A 12-year member of the BPD, Travis formerly was responsible for overseeing cases involving juvenile offenders and crime juvenile crime prevention education; however, as this research began, he changed responsibilities to oversee the BPD's Community Policing efforts.
- *Officer Dorance*. Has been a public servant in Belleville for over 35 years. He currently manages the 9-1-1 operators, in addition to his regular patrol duties.

Time frame

The collection of data began in June of 2008 with weekly visits to the BPD. The primary collection of data ran through the beginning of February, 2009. From August through January the researcher visited the BPD for 1-3 days per week in order to collect data. Following the initial phase of data collection, the researcher worked through late April of 2009 processing, synthesizing, and analyzing the data. The researcher finalized this dissertation in May, 2009.

Chapter 4: The Setting--Belleville

In many respects Belleville is typical of the towns and villages in its region (New England) and state. It was first established in the mid-1600s, during the colonial era. The town is located within 100 miles of four major metropolitan areas, including the state capital. It has over 15 miles of shoreline, as well as numerous inhabited and uninhabited islands. The shoreline community, during the late 19th and early 20th centuries, was a summer recreation area; however, today it is primarily residential. The town is intersected by a major interstate highway.

Although Belleville is primarily a residential community, it also contains retail, commercial, and industrial properties. The town's official census designation is 'Urban Periphery'.

Belleville covers an approximate area of 30 square miles. According to the official state data,[41] in most categories the town's demographic, educational, economic, and other socio-economic factors are representative of towns in the state. The town's population is between 25,000 and 35,000 with approximately half of the population counted in the active workforce. Demographically, the relative paucity of 18 to 24 year olds suggests that many are away in college; however the town's age distribution is otherwise consistent with the statewide statistics, as is true of racial breakdowns as well.

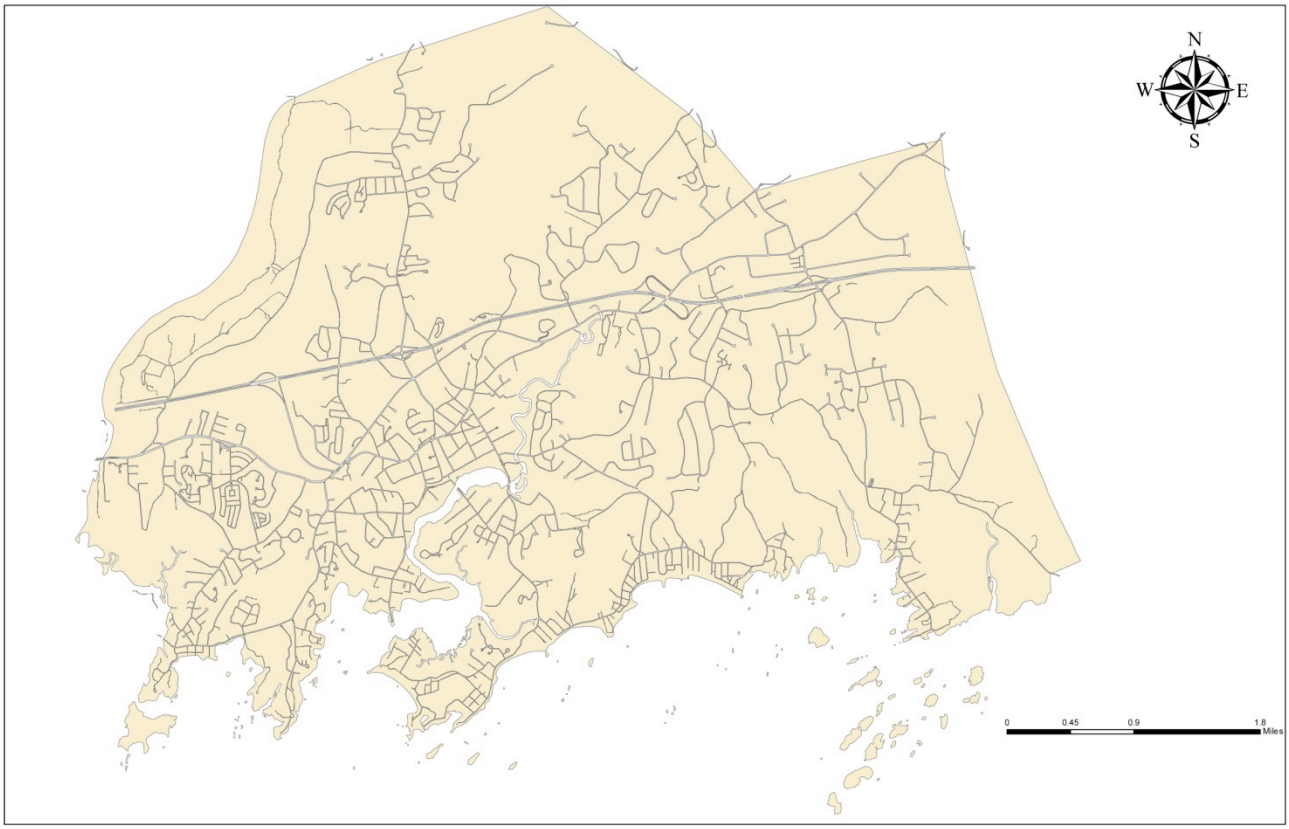
Certain economic factors are positively skewed. For example, the town's median income is more than $10,000 above the county median and close to $5,000 higher than

---

[41] Socio-economic data comes from the state's 2009 town profile data. Particular cite omitted to maintain Town anonymity

the state. The unemployment rate is almost a full point below the state average and the house median price is nearly $100,000 above the state median. These figures belie the fact that the housing stock includes multi-million dollar mansions along the shoreline as well as several trailer parks near the highways. That said, the percentage of owner-occupied dwellings as well as other housing variables mirror the statewide figures. Similarly, education factors are simultaneously skewed and typical. In statewide proficiency exams the students are well above average; however, their SAT scores are nearly identical to the state averages.

Illustration 3: Map of the Town of Belleville



Governmental organization

There is no functional county form of government in the state. The Town of Belleville is generally representative of the New England states in that it serves as the locus for political decision-making and operational service delivery to its residents. Within the state, a municipality may be operated either under the state's general laws, called statutes, or it may adopt its own charter. A town charter takes precedence over certain statutes. The Town of Belleville adopted its town charter in the mid-1950s.

There are three basic forms of municipal government in the state:

- Selectmen-Town meeting
- Mayor-Council
- Council-Manager

The Town of Belleville maintains a Selectman-Town meeting form of Government. There is a three-member Board of Selectmen and a thirty-member "representative town meeting." The first selectperson acts as the town's chief executive, creating a Weak-Mayor-Council type of government. Belleville has retained this form of government as other towns in the state have moved to a city manager or "Strong Mayor" form of administration.

The Board of Selectpersons thus acts in a fashion similar to an executive branch and the representative town meeting as a legislative branch, although there are variations to this general theme. In addition to the Representative Town Meeting and the Board of Selectmen, Belleville also has thirty-eight separate boards and commissions with over

250 members - some elected and some appointed - that oversee many town functions and departments, including policing.

Belleville Police Department: history and description

From colonial times and into the late 1800's many New England towns maintained a "night watch," a concept that the original settlers brought with them from England. Belleville began a part-time constabulary around 1900. Two town constables (with broad powers) were the sole peace officers. The nearby City of Old Gotham had started a police department almost forty years earlier. As Belleville continued to grow along with its policing needs, a six-member Board of Police Commissioners was created by a special act of the State Legislature around 1930. The Act authorized the Selectmen of the town to appoint each commissioner to staggered terms of service. The Board of Police Commissioners was tasked with organizing and maintaining a police department, and authorized to make all of the necessary rules and regulations for the control of the department. In addition, the commission was empowered to appoint officers, and to control, procure, and manage buildings and assets.[42] Immediately thereafter, the commission appointed the first chief of the department and the first six Belleville police officers.

---

[42] The current Belleville Board of Police Commissioners meets regularly on the second Monday of each month (with the exception of any month having a legal holiday on the second Monday of the month). Special meetings are scheduled whenever the business of the board dictates.

The Belleville Police Department (hereafter BPD) was originally located in the basement of the town hall, as was common in New England towns and villages at that time. In the late 1930s, the dozen full time officers moved into a converted former stable along with a contingent of ten part-time, paid supernumerary officers.

In the 1960s, the sworn members of the police department voted to become affiliated with the AFL-CIO for collective bargaining purposes. The only officers that remained non-unionized were the Chief and the Deputy Chief. In 1972, a former Old Gotham's Police Department inspector became the first chief appointed from outside of the department (a result of the mission to foster innovation in the agency). Since Old Gotham's Police Department had been aggressively adopting progressive modern policing tools and techniques, the new Chief's agenda also included reversing the perception that the "old boy" networks, favoritism, and selective enforcement had pervaded the BPD.[43]

The new Chief soon moved the department's forty-four full-time and fifteen part-time officers to a refurbished school building. In 1995 the BPD assumed the task of being the sole emergency services answering and dispatch point for the town. In this new role the department acquired a staff of eleven civilian dispatchers to coordinate the town's fire and emergency medical services, as well as police. That same year the department installed its first operational computer-aided dispatching and National Incident Based

---

[43] At this time there was a change in labor affiliation as officers voted to be represented by the International Brotherhood of Police Officers. This relationship held until 2006 when the labor union affiliation was again changed as Belleville officers chose to align themselves with a new labor organization called the State Organization for Public Safety.

Reporting System (NIBRS). Belleville became the first municipality in the state to submit NIBRS[44] data to the F.B.I. These changes necessitated a move into a facility specifically designed and built to accommodate both existing and newly added public safety functions.

In 2003, the department began the self-evaluation process leading to accreditation with the Commission on Accreditation for Law Enforcement Agencies (CALEA). Following the CALEA audit in 2006 the BPD was rated a 'level 1' agency (the highest rating).

Budget and structure of the Belleville Police Department during the time of this study

The total budget for the BPD is approximately $4.5 million. Just over 80% of the budget, or $3.6 million, goes toward labor costs (including over-time, insurance, and holiday pay). Currently, the budget supports 64 full-time employees and 16 part-time employees, and the BPD is nearly fully staffed at present.[45] The current patrol-oriented staffing levels are based on the classic reactionary approach to policing, which could become problematic given the BPD's newly adopted proactive policing strategy (see

---

[44] NIBRS (National Incident-Based Reporting System) is a modernization of the Uniform Crime Report (UCR). It greatly expands the number of incident codes from 10 to over 400, which provides more specific data about each crime. This program was piloted in the late 1980s and began in earnest during the 1990s. Agencies that adopt NIBRS are eligible for various federal law enforcement grants. Reporting data using NIBRS has been cost-prohibitive for many jurisdictions as it requires a flexible record management system.

[45] Technically, the agency is fully staffed; however, one officer is currently seconded to the DEA and another is on active duty serving in Iraq.

Table 3). The remaining 20% of the budget (approximately $700,000) goes toward capital expenditures, such as copiers, coffee, munitions, and gasoline.

The capital budget is deceptively small in light of all of the initiatives and use of technologies employed at the BPD. This is due to the fact that the agency transferred many of their infrastructure costs to the capital budget for City Hall in 2003. This includes most of their technology costs, utilities, and fleet maintenance. Also, since 2006 the BPD has actively converted asset forfeitures and sought external funding to finance their new initiatives (described below). These funds are accounted for "off budget" and are critical to the continuation of many of the implemented initiatives.

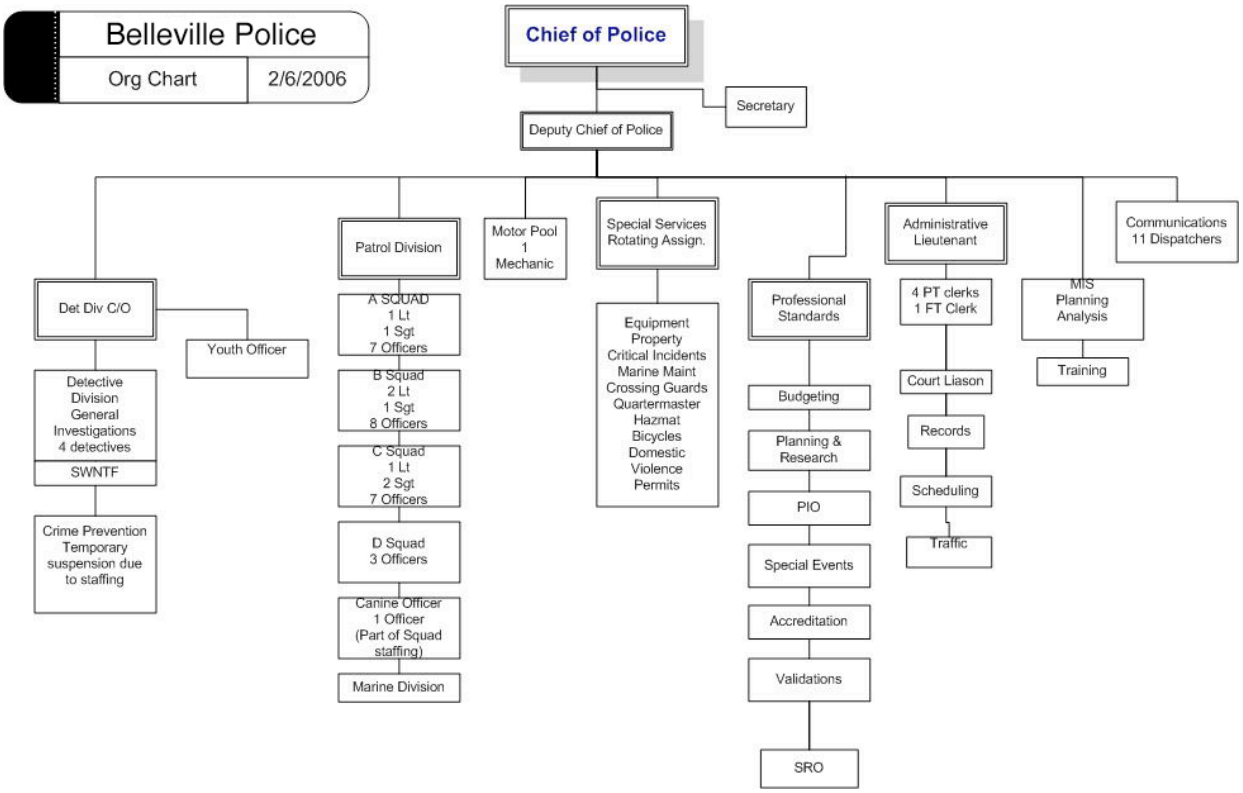
Table 3: Full Time staffing of the BPD

Sworn Positions	Quantity per position
Chief of Police	1
Deputy Chief of Police	1
Lieutenants	6
Detective Lieutenant	1
Sergeants	6
Detectives	4
Youth Officer	1
Patrol Officers	31
Non-Sworn Support Staff	
Dispatchers	11
Chief's Secretary	1
Records Clerk	1
Total full time Personnel	**64**

During the 2007-2008 fiscal year the police department handled 24,000 calls for service (CFS). Over half of the calls involve larceny or car accidents. Spillover crime from Old Gotham mostly involves drug and prostitution offenses. At current staffing levels the department provides mostly reactionary policing. The BPD's staffing is barely adequate for its many calls for service. Proactive programs to ameliorate crime rely on overtime work and/or grant money and asset-seizure financing. The typical Belleville citizen pays approximately $133 per year in taxes for police services.

During the time of this study, the BPD had one senior staff officer serving on active duty in the United States Army in Iraq. He cannot be replaced while he is gone. Additionally, a police officer had been seconded to the DEA. This benefits the agency through eligibility for asset forfeitures from drug arrests in the jurisdiction. However, the disruption in scheduling patrols due to the officer's absence is a problem. The BPD is currently reviewing this situation. The BPD also maintains a half-time School Resource Officer (SRO) by having one of the detectives work dual roles as a youth officer and a school resource officer. The officer previously working exclusively as an SRO has been reassigned to patrol to augment staffing levels in that division.

Illustration 4: Organizational Chart of the BPD



New direction for the agency

The current Chief of Police, Bernard Sowley, began his tenure in 2006 as the interim Chief. He officially became the 10th Chief of Police for Belleville in the spring of 2007. His predecessor ran the agency for approximately 10 years using a highly controlling management style. A photograph of the previous Chief (which remained on display until recently) showed him sitting at his desk, where a prominently displayed sign read, "'cause I said so." Not surprisingly, the agency operated under a *status-quo* mindset during his tenure. As a result of this approach, a number of issues festered, from recruitment to development of crime prevention strategies. Eventually the Chief was

asked to retire after it was discovered that he improperly used the city and statewide database for personal purposes.[46]

Upon assuming command of the agency Sowley sought to evolve the culture and structure of the BPD to better engage progressive and problem-oriented policing.

Sowley and the BPD today face numerous issues in professionalizing the department. One of the most pressing problems is that the pool of willing and qualified police applicants is shrinking. Background checks have become more extensive and sophisticated, thanks in part to DSTs, while qualifying standards have risen. Therefore, the BPD is challenged to make better and more intelligent use of recruitment and selection processes.

Labor unions, especially in the Northeast, have had a major impact on police management. Policies that were, or elsewhere remain, a prerogative of management have become subject to negotiation and formal grievance processes. The contractual entitlements of officers may put them at odds with organizational and community needs and goals. One area in which this occurs is in the scheduling of patrols. Labor contracts often limit or preclude department administrators from adjusting patrol and resource allocation without having to pay over-time salary. This directly impacts and reduces the flexibility needed by departments to divert resources away from the more traditional random patrols and focus them on a response model for crime prevention strategies.

State law prohibits police managers (as supervisors) and police officers (as supervisees)from being in separate bargaining units. This often puts police supervisors(sergeants and above) in the difficult position of having to discipline fellow

---

[46] The circumstances of his departure are covered in more detail later.

union members. In smaller departments this requirement often pushes discipline for all infractions into the hands of the most senior administrators.

According to Sowley this is one of the biggest hurdles in developing the culture and structure of the agency:

> "This [the reluctance of direct supervisors to discipline fellow union members] is counter to the simple management expedient of a scalar chain of command. It also precludes providing authority commensurate with responsibility and an entire host of other management principles. The efficacy of this situation, in light of building functional organizations, has really challenged me as an administrator. It has taken a lot of creativity to get the culture changed while not going outside of the labor contracts.
>
> Also, the content and quality of the future training that we provide our officers will become increasingly important in the future. As the population demographics of America continue to change, the diversity training that we provide at the recruit and in-service levels must increase - a move toward less militaristic and more community-centric. In addition, the pursuit of higher education by officers will ensure that our department remains a valuable asset... New and innovative ways must be found to facilitate the organizational and social changes that are called for by our law enforcement and order maintenance functions. An educated workforce will deliver on the promise that we have collectively made to protect and serve our community and continue to professionalize our chosen field of endeavor."

Major initiatives of the BPD during the time of this study

During the time of this study the BPD had initiated several programs in order to achieve the goals and objectives that Chief Sowley has established.

Community Oriented Policing and Problem Solving (COPPS)

One goal was that the department transition from the traditional reactive model of policing to a more proactive prevention-model. During the time of this study the BPD adopted the protocols of the Department of Justice's (DOJ) COPS approach.[47] To this end the department created a "Community Problem Solver" position within the patrol division by transferring Detective Travis to that division. According to Travis,

> "My job is to work with the different civic groups to identify community problems and develop specific plans for addressing them. Under the new COPS policing model, the department's mission was changed by the Chief to accomplish three goals: reduce crime, reduce the fear of crime, and reduce traffic accidents in Belleville. This is a clear, measurable, and easily communicated mission. If we keep this mission in mind as we make

[47] COPS is a specific protocol for crime prevention that is promoted by the DOJ and is based on the application of Routine Activities theory and Situational Crime Prevention mixed with elements of Community Policing. In short, it emphasizes community outreach and partnerships between police and the public in order to prevent crimes from occurring.

> decisions about the department we will remain progressive and still not forget the task we are mandated to accomplish."

To assist the transition to COPS, the majority of the BPD staff received training on Problem-Oriented Policing (POP) methodologies by an expert from the Regional Community Policing Institute (RCPI) at Michigan State University. The entire cost of the training and the salary of the department problem solver for 2008-2009 was subsidized by a federal grant. Since the COPS training took place, and during the time of this study, the BPD has seen promising results. Traffic crashes in Belleville have been reduced by 50% and the overall crime rate in Belleville has been reduced by 5%.

Neighborhood partnerships

In 2007 the BPD began holding neighborhood meetings in an effort to cultivate better relationships and address specific neighborhood concerns. One outgrowth of these meetings was the creation, in the summer of 2008,of Community Service Officers (CSOs). These CSOs are non-sworn personnel who address parking issues and provide a "police presence" in the neighborhoods and the central business district. Working with the Community Problem Solver and select command staff, they held community engagement meetings with the neighborhood stakeholders. The department also established a District Manager role. District Managers are primarily BPD Sergeants who maintain frequent contact with neighborhood representatives. The District Managers are held accountable for crime in their areas. They are also asked to develop initiatives and ideas on how to address crime and quality of life issues in their districts. According to the Chief,

> "By creating ownership of the problems in the communities by sworn staff at all levels, I have been able to get around the cultural problems that had built-up over the previous administration. Basically, my staff from top-to-bottom are having their perspectives on their job relative to the community shifted over time and through regular practice, rather than by compulsion or directives from "on-high." This approach has led to an increase in morale and, I believe, operational effectiveness of the agency".

In the spring of 2008 the BPD launched a bi-weekly television show on the local public-access channel called the 'Community CompStat Program'. This show, hosted by the Chief, brings in guests from around the community in an effort to bring the police-community partnership to the fore. The show communicates crime trends and concerns, and advertises the efforts of the BPD.

An important constituency in Belleville is senior citizens. The BPDS has established a TRIAD program, which is a partnership between the Belleville police department, a local bank, and the elderly community in town. The BPD has tasked an officer to this program who liaisons with the partner groups to address victimization and safety issues involving the elderly. During the winter of 2009 the BPD conducted a survey of the elderly in town, which led to an expansion of the TRIAD "Yellow Dot" program. The "Yellow Dot" program was created to help senior citizens who are involved in an automobile accident. Participants receive a yellow dot sticker to place on their windshield, which alerts and authorizes emergency services personnel to look for a

corresponding yellow folder in the glove compartment. The folder contains current medical information, a photo, hospital preferences, and contact numbers in case the senior citizen is not able to communicate.

Crime Analysis and COMPSTAT

In the spring of 2008 the department began a crime analysis project utilizing student interns from the University of Old Gotham. These interns mine the department's database for 'hidden' crime patterns and propose strategies to address the crime trends. This analysis provides the command staff with timely and accurate crime information that is distributed and discussed at weekly CompStat meetings. One strategy employed is the use of police Matrix teams. These are special teams that operate in conjunction with the Community Problem Solver to mitigate crime and disorder. Instead of merely reacting to and reporting crime and disorder, the Matrix teams focus on solving underlying criminogenic and order-maintenance issues.

Other technological innovations

The BPD has generally taken a proactive stance towards the incorporation of new technologies available to police departments. In conjunction with Belleville's IT department and other Belleville agencies, the BPD implemented the 'Code Red' system in the summer of 2008. This system allows participating departments to send out mass phone messages to specific areas of town in the event of an emergency. The BPD was also the first police department in the state to offer near real-time crime information to citizens through Crimereports.com. This is a free web-based system that the residents of Belleville can access via the internet.

Also in the summer of 2008, the BPD began offering citizens and businesses alerts through a corporate grant provided by Alcoa Howmet. This program, called "Be Alert", is for those who volunteer to receive alerts from the BPD through email or cellular phone text messaging. The alerts include Amber Alerts regarding missing or abducted children, crime notifications, and emergency management notifications for events such as flooding. Individuals can sign up for the alerts through the BPD website.

During the summer of 2008 the BPD began installing surveillance cameras throughout the jurisdiction. This includes both fixed cameras in the Stony Creek neighborhood, as well as mobile cameras that are connected through wireless internet. Stony Creek is a high traffic area in the summer due to tourism. The mobile cameras allow for the surveillance of particular locations to assist an investigation or as part of a particular crime prevention initiative. The cameras have helped to solve several major crimes, including a bank robbery.

Officer and management training and succession planning

When he took command of the agency in 2007, Sowley realized that he had an ambitious agenda and that if it was going to work, he needed to get his executive staff on-board. Beyond that, he realized that his time as the Chief was not going to last "forever". According to Sowley, "A really good manager surrounds himself with the best people he can, and finds opportunities to promote their development". In the end, he felt that his greatest mark would be to position his command staff for promotion within the BPD or to become chiefs in other jurisdictions. As he says, "Their success is not my failure… which is an attitude, I believe, a lot more police managers need to take on."

To achieve these possibilities for both the command and junior officers, the Chief implemented a number of new initiatives. During 2008-2009 nearly all of the BPD's first-line supervisors attended a comprehensive, two-week course of study at Roger Williams University. Two of the command staff members attended the exclusive and academically challenging Senior Management Institute for Police (SMIP), provided by the Police Executive Research Forum (PERF) at Harvard's John F. Kennedy School of Government. During the winter of 2009 a command staff officer attended the FBI's prestigious National Academy, and another is slated for 2010.[48] In the summer of 2009 another command staff member will attend graduate level courses at the Southern Police Institute (SPI) at the University of Louisville. The SPI is a regional version of the National Academy and is available on a more frequent basis. Lastly, four command staff members are currently completing graduate-level criminal justice degrees, with scholarship support from the city.

The Chief has undertaken a significant change in the leadership of the BPD. All of the division heads, with the exception of the Detective Bureau, were re-assigned. For example, the heads of Administration and the Patrol Division switched roles. This was something that the Chief had planned but did not tell anyone about until a week prior. Each lieutenant was moved away from an area that from experience or inclination was in their "comfort zone". This initially caused some discontent; however, that eventually faded away. The point, according to Sowley, was "to not let anyone get stuck in a rut… if

---

[48] This is unusual. Typically, a department the size of Branford gets a National Academy 'slot' once every 7 years or so; however, the Chief has developed a good working relationship with the state authority that approves these appointments.

you want to be a Chief or Deputy Chief you have to be comfortable in leading people throughout the organization. You have to understand from experience how various operations function. Then you will earn the respect of the lower ranks and they will more easily take your new ideas and your direction".

During 2008 the BPD procured, for the first time in 15 years, a working firearms training range. When fleet maintenance responsibilities were transferred in 2007 to the city, the BPD was able to convert its old mechanics' garage space. Funding is provided by the town, as well as by asset forfeiture monies due the department. The range is state of the art and includes video scenarios to help improve marksmanship, as well as training in the proper use of force.

Use of Force Alternatives

In 2008, the department purchased Tasers (Conducted Energy Devices, or CEDs) and trained officers in their use. Asset forfeiture funds were also utilized for this program. The Tasers give the officers an intermediate option for the use of force in violent situations.

Training for future officers

Not everything has gone according to plan. An attempt at a part-time police academy went back to the drawing board. This would have trained recruits on the weekends for a two-year period while allowing them to work during the week. The benefit of such an approach includes cost savings and a broadening of the applicant pool. Normally it costs $32,000 to send a recruit to the academy; the estimated cost savings of the weekend academy is nearly $16,000 per recruit. The academy planned to begin in the

fall of 2008. During the spring and summer of 2008 the BPD processed 150 applicants. Fifteen applicants had to make it through the background, physical, psychological and polygraph exams in order to make the part-time academy cost effective; however, only 10 of the 150 applicants qualified. Sowley and his colleagues are planning on pursuing the initiative again in 2010 in partnership with a neighboring jurisdiction in order to achieve the critical mass of recruits.

Visible Changes

According to Sowley "Part of changing the culture means changing the way we dress and look… to that end, I wanted to make our uniforms and patrol cars 'cool'." In 2007 Sowley asked some of the patrol officers to form a committee to design and modernize their uniforms, cruisers, and departmental logos - which had last been done in the 1970's. This has proved popular with the staff- As one patrol officer remarked "we now look like the type of agency you would see in a TV show- it's cool". Also, friendly competition among the staff over whose design would win boosted morale. In the summer of 2008 the BPD began to implement the new uniform and car designs.

Chapter 5, Longitudinal findings: Development of DST's in Belleville

1970's CIFRS [Crime Incident File Reporting System]

Connchusetts county governments do not have the ability to direct or fund police programs. Because each city, town, and village is largely on its own, regional initiatives require a lot of cooperation between agencies. During the 1970's, with federal funds from The Omnibus Crime Act, the Old Gotham Police Department constructed the first region-wide digital records management system in the state. This system was meant to streamline data sharing between the 13 jurisdictions of Old Gotham County, and was called the Crime Incident File Reporting System (CIFRS).

The construction and maintenance of CIFRS was centralized within the Old Gotham Police Department. The system was designed to be housed on an IBM System 3, a punch card-based system. All original records of arrests and initial dispositions were done by hand in the participating departments. Dispatching was conducted by police officers assigned to work a radio detail. Data that was to be collected electronically in the central system had to be submitted on standardized forms to facilitate punch card entry. Thus, each jurisdiction would send a daily shipment of its original police reports to the NHPD, where they would be transcribed onto punch cards. The punch cards would then be entered into the system.

The data on each punch card was standardized tabular data from the crime report forms. This included 27 different fields, such as when and where the offense occurred, as well as victim/target data and offender data. However, this did not include the non-

tabular (descriptive/narrative) data included on the original police report. Thus, any non-standardized details that might be critical in terms of pattern analysis and M.O.'s from different offenses was not initially shared. Also, data about case subsequent dispositions or any other relevant updates had to be done by punch card.

All of the data was stored in Old Gotham. Once the information was stored on the network, it was retrievable from within each jurisdiction. Each police department had a single Raytheon "green screen" or "dumb" terminal. These terminals did not store any data locally nor did they log usage. They could only "call up" data from the central database. They were called "green screens" because they were typically black screens with green text and did not have the ability to render images; the entire network was connected by dedicated, and slow, data lines.

Illustration 4: Example of a 1970's era IBM "green screen" terminal

The capacity of the initial Crime Incident File Reporting System [CIFRS] system soon became a critical issue. In the early seventies as today, the BPD fielded between 22,000 and 26,000 individual calls for service, about 40% of which required a police

report. Belleville's population during this time was approximately 30,000. Other towns in the CIFRS consortium were larger, including Mintchester (60,000), North Gotham (80,000), and Old Gotham (140,000[49]). With thirteen jurisdictions sending cases to Old Gotham for data entering every day, the load soon became unmanageable. The backlog of cases not yet entered grew exponentially, so by the time cases made it into CIFRS, there was a high probability that the next stack of forms contained new information pertaining to cases just entered.

The System 3's punch card technology required more personnel than had been planned for or budgeted. The budget for the system had not considered the amount of dedicated staff required to keep the system updated. The punch-card system required two to four fully-tasked clerical staff; however, only one person had been budgeted. A several week backlog of unprocessed cards became the norm. Over time, data accuracy progressively degraded with overloaded core and temporarily assigned staff unable to keep files accurately updated

By 1978, the System 3 was replaced with an IBM System 34, which brought much-needed improvement. Most importantly, it ended the need for punch cards. Secondly, the data could be entered and edited directly from within the individual terminals available in *each* jurisdiction. Third, diligent entering and timely editing allowed police agencies in the county to maintain a near real-time distributed data network of accurate crime data.

---

[49] Population estimates for the towns in Old Gotham County have largely been static since the 1970's with the exception of Old Gotham which, according to the US Census Bureau, has seen a modest reduction.

The data in the system was designed around individuals. The primary data points for identifying individual A versus B were the name and date of birth. When there were multiple individuals with the same name and birthday, race and other physical descriptors were used to differentiate.

"Crime doesn't stop at the city borders"

Connchusetts state law, circa 1978, was largely directed toward pre-trial release or using alternative sentencing for first-time offenders, absent any evidence of prior illegal acts.[50] However, unless the police or District Attorney could obtain records from all of the other jurisdictions in the region, there was no way to accurately establish an individual's criminal history. CIFRS was an elegant solution to this and other problems law enforcement had to deal with, and allowed a more effective and state compliant law response to crime.

CIFRS was an exceptionally valuable regional tool. It compiled a massive amount of data from numerous police departments into a common database. According to Sowley,

> …the criminals didn't stop at the town line and our town lines are relatively on top of another. We would get the goods on people who had lengthy criminal careers throughout the region. With CIFRS, the biggest strength was the ability to track down data on the individual.

CIFRS was quite advanced for the 1970's because it provided region-wide data. For example, if a user in Belleville entered the name "Thomas M. Kelley," CIFRS would

---

[50] For a fuller discussion on this topic, see (Feeley, 1979).

return all contacts[51] under that name for all police departments in CIFRS since the inception of the system. "Contacts" included everything from arrests to victimizations to investigative questioning. Also included were traffic stops from all participating jurisdictions that resulted in a summons or a warning.

In the late 1970's the federal data repository, called the NCIC (National Crime Information Center), was still a concept. Connchusetts, however, was creating its own statewide data repository named COLLECT (Connchusetts On-Line Law Enforcement Communications Teleprocessing system). The regional CIFRS system was upgraded to connect to COLLECT soon after it came online. Police in Belleville and surrounding towns could retrieve two kinds of data about an individual: warrants and DMV data.[52]

The demise of CIFRS

By the end of 1980, the five-year CIFRS experiment was discontinued by Old Gotham. The primary reason had to do with procedural difficulties and resource limitations related to data maintenance and upkeep. The underlying reason was an impasse over resource allocation and cost-sharing among the participating jurisdictions.

The fatal weakness of the CIFRS was that although departments were excellent at entering information they were lousy at maintaining it. According to Sowley, "…once the data was put into the system the data has to be maintained and updated. At this, almost all the agencies were very poor." One example of this is the adjudication and disposition of a

---

[51] A "contact" in this case refers to any interaction between law enforcement and the individual - including traffic violations and calls for service initiated or involving the citizen,either as a reported victim or offender.

[52] However, this was limited to suspension and automobile registrations.

given case. The police would file one charge and later, at court, the charge would be pleaded down, dismissed, or adjudicated "not guilty." A recurrent problem had to do with *nolo contendere* (no contest) pleas. In Connchusetts a '*nolo'* plea on a misdemeanor was viewed as a *temporary* finding of guilt. If the individual did not engage in criminal activity for 13 months, then the charge was dismissed. At that time "not guilty" became the finding of record.[53] By law, all data pertaining to a '*nolo'* plea was then to be expunged by the local (originating) police agency from the computerized records. Another recurrent problem involved individuals "wanted on a warrant," whose status was not changed by the police agency after the warrant had been served on the person.

These and other changes often were not made. Erroneous information stayed on file, due to limited clerical staff, data entry errors, ad-hoc processes, and fumbled information transfers between police and judiciary. The amount of illegitimate information left in the computer files by most departments was substantial.

On the other hand, Belleville was well-staffed and had created a workflow process to support CIFRS updates. As a result, the BPD was able to keep up on a daily basis with modifications to the system and the expunging of data such as the *nolo* findings that had, as a matter of law, changed.

Unfortunately, Belleville alone could not cure the data problems endemic throughout the system. As Sowley explained, "There was a meeting of representatives from all of the participating agencies in mid-1980. It was very clear from that meeting that there were very different understandings of how to proceed, given the totality of the circumstances." Other issues raised at that meeting included a lack of understanding of

---

[53] For a dismissed case to be also expunged from the record required a formal request made to the court.

who had post-adjudication record correction responsibilities - the police or the court. Also, the police argued that they were neither trained nor funded to edit records in the system. Whatever the reasons, the data maintenance problem had only been increasing with time. This also meant a growing potential liability due to misinformation that could compromise an individual's reputation, liberty, or civil rights.

The system had in fact degraded to the point where citizens were being held or detained based on erroneous information with increasing frequency, especially when data in the system originated in the larger jurisdictions in the consortium, especially Old Gotham. As one veteran officer stated, "I personally had several cases where people where I picked people up on warrants who later had to be released because, although the information in the computer said that the warrant had not been served, it actually had."

Officer Dorrance, a 40 year veteran of the BPD and who currently oversees the civilian dispatchers stated:

> It was well known… the problems with the information being incorrect on cases. It was not uncommon to hear about situations where someone who was picked up because the system said so… later had to be released. These problems would be rectified by contacting the jurisdiction where the originating incident occurred and asking them to look in their local files for the latest information on the case. Of course, this was disruptive for citizens and it did defeat the purpose of having CIFRS in the first place.

Each jurisdiction's prosecutor had a different protocol for determining when an arrest was erroneous. Sowley recalled that at the 1980 meeting, "…there was even discussion about how, or if we could, 'unarrest' someone who had been erroneously

arrested or if we (the police) should let the prosecutors and the courts deal with it." He also went on to explain that the administrators were worried that someone might litigate over one of these situations. "We weren't so worried in Belleville; however, the larger jurisdictions were and that was obvious from the conversations you would have with them…."

By 1983, with Old Gotham's benign neglect, the attendant processing difficulties, and the possibility of legal liability from false arrests, individual departments in the CIFRS consortium began to opt out. By 1985 the whole CIFRS consortium had fallen apart.

CIFRS was neglected by some agencies, unevenly administered by all, and confronted an increasing data load with static resources. Only Belleville retained the operational capability to carry on if CIFRS, or a successor, was to be revived.

Mid-1980's, Ad-hoc Digital Record Management System

After the demise of CIFRS, Belleville went about creating a localized version for its own needs. The new system was a digital record management system [RMS] that would service and contain data generated by the BPD. This system was built and maintained by two police officers, one full-time and one auxiliary.

Both officers had unique backgrounds that made them particularly suited for this task. The full-time officer, Detective Sowley, had a B.A. in computer science. In the early eighties he had been seconded to the FBI to work on counter-espionage cases involving theft of U.S. technologies by Soviet agents. Even while working full-time for the BPD, he

maintained his programming skills and kept abreast of public and private sector data solutions. He was eager for an opportunity to use his skills in Belleville.

Sowley's enthusiasm for policing data solutions was matched by Belleville Auxiliary Officer Arendosh, who worked full-time as a computer software developer for a financial services firm in New York. Both Sowley and Arendosh worked at the BPD during the time that the CIFRS program was active, and they both understood the power and weakness of that system.

"We wanted continuity with the old system and control over the data… so we created our version in-house that collected the same information and, for the user, worked in the same way as the old CIFRS - with one critical difference - it only contained BPD data," explained Arendosh.

Being a relatively small agency, Sowley and Arendosh realized that Belleville was too small an agency to obtain a level of equipment comparable to what had been utilized in CIFRS. In 1984they started experimenting with microcomputers and local data storage equipment and began writing programs to exploit that hardware using the BASIC computer language. Version 1.0 of their new program was useful but extremely rudimentary. The program tracked motor vehicle accidents and call for service [CFS] incidents. Next, Sowley and Arendosh utilized VisiCalc spreadsheet software (that later became Microsoft Excel) to do basic data analysis of the digital records. Their work directly contributed to the BPD's decision to commit to the new IBM PC's as a core hardware platform for data analysis and office productivity.

The BPD began to record crime data in the IBM computer using indexed sequential access method (ISAM) files, a carry-over from the old magnetic-tape based

mainframe. This approach did not take advantage of the non-linear recording capacities of the desktop computers' internal hard-drives, and was a relatively slow and inefficient approach. Nonetheless, at the earliest stages of development, ISAM was sufficient.

As the system was organized, an officer would type data into a word processor called Bank Street Writer (a precursor to Microsoft Word). For tabular data(dates, times, addresses, names, etc.) an in-house database was created by Sowley and Arendosh. Within a few months, the BPD outgrew the storage capacity of the personal computers. The Chief at this time, who championed the work of Sowley and Arendosh, authorized the acquisition of more computer assets in order to effectively evolve their in-house system. The BPD acquired an IBM Model 36, which was a network-based business computing platform, similar to the one employed in the regional CIFRS system. Now, however, these resources were focused on Belleville alone.

This computing power allowed Sowley and Arendosh to fully develop the BPD's in-house system. This stand-alone system removed the dangers associated with having to use other agencies' inaccurate or corrupted data. However, the abandonment of the region-wide CIFRS also removed a major benefit. As one veteran officer, who was familiar with both CIFRS and the in-house system remarked, "It was invaluable to be able to share data because, obviously, criminals do not operate in only one jurisdiction. What we gained in data integrity (with the stand-alone system) we lost in data richness."

1990's Systematizing the data collection

From around 1985 through the early to mid-1990's Sowley and Arendosh concentrated on perfecting and maintaining the system that they had created. Two successive chiefs over this period remained supportive, but also made sure to align their

activities with budgetary imperatives. Sowley and Arendosh were not permitted to work on developing new software for the system during business hours. Their positions were budgeted for enforcement purposes. Anything they did to fix, maintain, and upgrade the system had to be done "off the clock." Thankfully for Belleville, Sowley and Arendosh viewed working on the system as both an exciting experiment and a labor of love. At the same time, the departmental administration was setting aside an increasing amount of the BPD's capital budget in order to maintain the hardware and acquire new assets.

The administration "bought in" to the system in terns of capital expenditures, but could not spare the manpower to staff the system. Though this seems a halfway measure, it did help move the system forward, which was certainly not the case in many similarly-sized and situated police departments where little was done except wait for new systems to be established by others, as Old Gotham's CIFRS had been to the benefit of surrounding jurisdictions.

Neither Sowley nor Arendosh know precisely how much time they spent building and maintaining the system. They do recall weeks where they were working as many as forty hours on the system in addition to their full-time jobs. Their "above and beyond" contributions are in stark contrast to stereotypes of civil servants who "do the minimum." The value of their time, at the prevailing rates for software and network developers, over the ten years that they were the de facto managers BPD's RMS, would have exceeded $500,000. Without their pro bono work, the BPD could not have built the system. To illustrate this point, one need only consider Old Gotham's attempt to get back in the RMS game in the mid 1990s. Old Gotham purchased IBM's top-of-the-line mid-level data server, the AS400e. However, the server sat in its crate for almost 4 years because Old

Gotham could not afford the cost of paying consultants to develop the necessary software, nor the cost of the infrastructure needed to house and support the system.

It is not uncommon in cash-strapped jurisdictions to make investments in technology solutions without adequately considering the total costs of such a project. Both Sowley and Arendosh agree that their incremental approach in patching together systems and equipment provided them an invaluable foundation for understanding RMS functioning. They were on the cutting-edge, unbeknownst to anyone outside of the BPD (and sometimes to themselves). However, their belief was unwavering that the system would have major pay-offs down the road.

In 1994 Sowley's and Arendosh's work did pay off with a major investment by the department and city administrators. The city had agreed to combine all of the city's emergency services into one operations center. Dispatching for fire, police, and emergency medical services would be done from that center.

This was a significant change in many respects. Previously, dispatching was done by police, fire, and emergency personnel who were rotated through that task. Since the dispatchers were familiar with the needs and demands of particular emergencies, they could rely on their experience to appropriately direct which of their unit(s) needed to be involved. They also knew from experience when and in what manner they would have to get other services involved on a particular call for service. Each service had its own dispatch system, the dispatchers would have to call each other in different locations and play a game of "radio telephone" in order to coordinate. This system was clumsy and fragmented. However, the professional skills and intuition of dispatchers, to some degree,

offset the inefficiencies. Also, while the service area was large (approximately 24 square miles), the moderate call volume helped make this system workable.

Civilians, however, would staff the new dispatch center. Most dispatchers would not have direct emergency services experience. All dispatchers would work from a centralized location, run by the BPD, which fielded all emergency calls for service.

Consolidated dispatch addressed the inefficiencies of the prior departmentalized model. However, the reorganization made for new problems. Combining the services into one call center would mean that there would be a larger volume of calls of a greater variety - from burglaries to house fires to cat in a tree.

The city realized that they would have to significantly expand the capabilities of the RMS to accommodate the range of different records made by fire, police, and EMT services. They also would require a computer-aided dispatch system to efficiently handle the increased volume of calls.

Sowley and his colleagues were directed by the city and agency administrators to find a solution. They quickly realized that they were not equipped to create an integrated RMS. There was no time for decade-long, labor of love development. Viable integrated solutions were on the market. Thus, Sowley and his colleagues endeavored to find outside vendors.

The search for a new system began in earnest in early 1994, about a year before the transition to the new police building with centralized dispatch. Sowley conducted a national search for the right vendor and seriously considered about five of them. The key criteria was whether or not the vendor had implemented a system for jurisdictions that

were roughly the same size as Belleville, and whether or not their system could be customized for the peculiarities of the coding system used in Connchusetts.

The chosen firm had, to that point, conducted over 140 individual installations for police agencies in Texas, Iowa, and the D.C. Metro area. The vast majority of their clients were similarly situated to the BPD, and this increased confidence. The firm, Applied Micro Technologies (AMT), had about 100 employees but the operations were run directly by the founder and CEO. There were several factors about the AMT approach that worried Sowley and his colleagues, but the town administration overruled their objections based on cost.

The biggest concern had to do with customization. No vendor, at that point, had implemented an integrated RMS/dispatch system using the Connchusetts regional service codes. However, Applied Microtechnologies wanted to customize their system for the BPD so that AMT could then turn around and sell the same system in the region. In other words, the vendor was undercutting the price to get the account in order to get future sales. During that era, the typical police agency in the U.S. used the basic Uniform Crime Report (UCR) coding for their records, which had 10 different categories. In the 1970s, when the BPD joined the CIFRS project, they adopted the Old Gotham Police Department coding system, which had 400 different categories. Moreover, in 1995 the BPD became the first Connchusetts agency to adopt the National Incident Based Reporting System (NIBRS). This meant that their new system would have to port over their existing data and transpose the codes. In short, Belleville wanted a system that allowed for continuity with their existing dataset.

There were other challenges as well. The system would have to handle police, fire, and emergency service data, each with their own unique codes. The code structure in Connchusetts and the surrounding states was more complex than that used in the rest of the United States where AMT had clients. Most AMT clients used 10 codes that mapped to the UCR. Conversely, the BPD employed about 400 different call types designed to facilitate more detailed reporting and analysis, and support resource deployment decisions. Whatever system AMT developed had to be able to port all of these codes. This was important in order for BPD to migrate all of its collected data from their existing system to the new system.

As AMT delivered the new system, the BPD began to submit data to the National Incident-Based Reporting System (NIBRS). NIBRS is an update to the antiquated UCR system of categorizing and storing data that was initiated by the FBI in 1929. Providing the data to the federal government in the NIBRS format made the agency eligible for certain federal grants. Moreover, it gave the BPD the ability to share with other NIBRS reporting departments.

Since the AMT system was only designed to handle police calls for service, the integration of the police, fire, and EMT dispatching required additional customizing. For example, at that time, the fire department was mostly comprised of volunteer firefighters. Each member, including volunteers was notified by an elaborate pager system when there was a fire service. The paging was supposed to be automated through the AMT dispatch system; however, it never worked properly. As a result, a new ad-hoc pager and radio communication system was built by Officer Dorrance, who had expertise designing and

managing radio and pager technologies and who, in addition to his BPD responsibilities, was also a volunteer firefighter and EMT in Belleville.

Another problem, which affected all of the services differently, concerned the pre-determined responses to particular CFSs, called “running orders.” Since the dispatchers were not professional police, the system needed to guide them in making the right decision. Thus, the logic of the “running orders” needed to be encoded.

For example, the police department required an automated way of dispatching cars based on the particular number of patrols on duty during a given shift, as well as the location and particulars of the call. For a “breach of peace” or a “domestic disturbance” call, the normal protocol was to send two cars - one from the sector of the call and another from next closest sector. However, if either patrol was servicing another CFS then dispatchers needed a mechanism to determine what other units should be sent. A “fall through” algorithm was needed whose logic included beat patterns within the town, which varied at different times of the day and on different days of the week. Sowley and Arendosh worked with the vendor to incorporate this algorithm in the running orders dispatchers used.

When the BPD moved into their new dispatch facility they launched the AMT software. It was the first time in Connchusetts that a computer-aided dispatch system and a records management system were tied in to one another.

This feature of the system included a common thread (each CFS was designated a unique identifier number) for a case from the first time that it was called into a dispatcher all the way through the subsequent processes. The unique identifier also facilitated the aggregation and reporting of crime data to relevant federal or state authorities.

As an individual call came into the system it would be assigned a call type, and the appropriate resources would be dispatched to the call. The dispatcher could determine a large amount of information from the person making the call. Before the responder arrived at the scene, the following information would be captured and encoded into the system: address, name, and the circumstances of the call; additionally, if call came in via911, the system could automatically identify the owner of the incoming phone number, as well as the known location of that number.

On a police call, once the car was dispatched the officer would go to the call, and at the conclusion of the response, would code the call with what is called an "actual call type," and then write a report. This actual call type was the final disposition by the on-scene responder, as opposed to whatever initial call type the dispatcher applied based on the CFS. The initial code would often be less accurate in describing the situation.

As early as the 1960's the BPD did not allow officers to hand write police reports. This served two purposes; to control for problems with illegibility, and to improve quality control for reports. In 1989, the BPD issued each officer a portable micro-cassette tape recorder. Each officer would dictate a report in the tabular format of the Old Gotham incident reporting system, and then recite the case narrative. Each officer, using a micro cassette recorder, followed a prescribed script when dictating his report (see Appendix A).

The use of a consistent script made transcription more efficient. Also, using the tapes made it much easier for supervisors to control and monitor the reports. The audiotapes went into a typing pool, where clerks entered the data and prepared the reports. The officers then reviewed, edited, and signed-off the reports which then went

back to the clerks who corrected minor grammatical errors or misspelled words. This quality control, enabled by audio reports, became even more valuable after the BPD began submitting data to NIBRS.

A new venture

In 1996 the CEO of AMT, Tom Marshall, asked both Sowley and Arendosh to leave the BPD and join AMT. Both of them seriously considered the offer. However, they each decided that they had too much invested in their current positions and did not want to uproot their families. They did, however, agree to work on a contractual basis as consultants. They would program new features and functionalities and help implement and install systems at AMT's client sites. This gave both of them access to the source code of the system. The original AMT system was built using a programming language, BASIC, which was already archaic by 1996 standards. In fact, the basic code was already an upgrade, as the system had originally been developed in another computer language.

Having access to the source code and working with so many different jurisdictions (including agencies in Georgia, Texas, California, and Tennessee) gave Sowley and Arendosh a lot of insight. Seeing the needs of various agencies, both large and small, as well as their different legal and procedural requirements, this experience became another valuable addition to their already formidable expertise with police RMS. In 1998, the CEO of AMT died unexpectedly of a heart attack. This put the firm, as well as its clients, at risk. The firm's decisions were centralized through the CEO, and AMT

had just begun to plan the necessary steps to migrate their systems past the Y2K problems.

Soon after the death of the CEO, AMT was purchased by a data management firm out of the U.K., Memex Corporation. Memex was an intelligence gathering company in the UK, and they were building social networking intelligence software for the British domestic and foreign intelligence agencies, MI6 and MI5. Memex soon decided that it no longer wanted to be in the business of providing data management products and services to police agencies in the U.S. and pulled out of the market. This meant that all U.S. public safety agencies that were using AMT software were on their own in maintaining their systems - a key service that AMT had previously provided.

Sowley and Arendosh saw this as an opportunity. Both men were intimately familiar with the system and knew what it would take to port the pre-Y2K system over to a Y2K-compliant one. Also, both men have an entrepreneurial spirit and wanted to start their own company. They began negotiations in 1997 to acquire ownership of the source code to the AMT system. Their intention was to approach the over 140 now abandoned AMT clients and build their own enterprise from there. As the negotiations continued, it became clear to both Sowley and Arendosh that the task of taking over the existing corporation and obtaining the financing necessary was a larger project than they were prepared to take on at that time.

At the conclusion of the negotiations, Sowley and Arendosh set their sights on a more modest venture. They instead decided to approach the local agencies that had implemented the AMT system about providing ongoing customer service. Thus, they worked in their official capacity by servicing the BPD’s system but, as private citizens,

provided a consulting service to four other agencies in their region. Consequently, in late 1997 their two-person firm, "NextTech," was founded.

Like their shared experiences working for AMT in developing and implementing their software, this new experience allowed them to experience, in a limited way, the practical realities of running their own business. They also discovered that servicing a complex information system built with antiquated code was far more complicated than they anticipated. Each of the agencies had demands that the system was not designed to easily accommodate. The best example had to do with the existing system's lack of generating reports for analysis and, more importantly, NIBRS reports. In the 1990s, police agencies around the country were beginning to adopt COMPSTAT or similar models of local data analysis. The purpose was to prevent, rather then respond to, crime by directing resources to geo-temporal crime "hot-spots." Also important for agency administrators was access to federal grant money associated with supplying NIBRS compliant records.[54] Unfortunately, the underlying logic of the original system was primarily as a digital warehouse of data, rather than a sorter and disseminator of operationally useful information.

Given the challenge of scaling the existing system(s) to meet these new demands, Sowley and Arendosh decided to build their own system from the bottom up. After all, they reasoned, they had done it before with less efficient technologies than they now had access to in 1998. They both had, moreover, worked for the previous two years from the inside-out on a complex, multifunctional RMS that was considered state of the art. The totality of their previous 15 years experience with bottom-up systems development and

---

[54] This is addressed in more detail below.

their experiences of the past two years customizing an "off the shelf system" convinced them that the time was right.

Public-private-public partnership

Sowley and Arendosh approached the Chief of the BDP in late 1998 with a proposal to fully develop and implement, in-house and from the ground up, a new RMS and computer-assisted dispatch (CAD) system that could handle all first-responder services and related data management and analysis needs. Their idea was to use Belleville as a testing site where they could develop and implement their concept. One of the keys for them was that they wanted NextTech to own the rights to sell that system to other interested agencies. In this way, a partnership would be created between the BPD and NextTech. There was the potential, immediately recognized by all people involved, that this partnership could appear to involve a conflict of interest. Although the Chief wanted to promote innovation, he made it clear to Sowley and Arendosh that they, as NextTech, had to agree to the following conditions:

- There was to be no outlay of costs for the BPD that would not be normally assumed by the agency. Thus, the agency would purchase the necessary hardware or software to use the system *but would not provide the funding to create the system*.
- No official time was to be spent on the project, even for implementation and quality assurance (QA). All time spent on this project by Sowley and Arendosh had to be on their own time. To document their compliance, both Sowley and Arendosh maintained highly detailed logs of their efforts.

- During the development of the new system, both Sowley and Arendosh had to maintain the existing AMT system.
- Once the system was up and running, future updates and "normal" evolutions of the system were *gratis.* This was important because Sowley and Arendosh's initial plan was to create a subscription model, whereby the other former AMT clients would be offered the initial system at no cost and then pay a yearly service fee to cover the costs of normal updates and maintenance of the system.

The BPD benefited from this relationship in several ways. Importantly, the agency received a fully customized RMS and CAD that supported the specific data demands for all of the town's emergency services. Secondly, the new system integrated with their existing pager and telecommunications systems. Lastly, the cost of creating a similar system with a technology consultant would have cost upwards of $500,000- an amount that the town could not afford.

Sowley and Arendosh decided to name their new system "LEAS" (pronounced "Lee-ah-s"), which was an acronym for "Law Enforcement Administrative System;" however, between them they referred to their project as the HAL 2000, in reference to the homicidal computer in Arthur C. Clarke's and Stanley Kubrick's 1969 movie "2001: A Space Odyssey." As Sowley stated,

> …working on the project was the equivalent of a third full-time job. I was a senior detective with a full case-load, a family, and this idea. But, what would happen is that I

> would go home and work on LEAS in my basement until one or maybe three in the morning…. To amuse ourselves we started referring to the system as HAL, after all, we were coming up on 2000 and to keep myself awake at night I would speak to the computer. Also, 'HAL' was really buggy at first and at times it felt we were perpetually in the in the scene from the movie 'Space Odyssey' where the computer is trying to sabotage and, in fact, kill the humans. There were times where we wanted to take an ax to our own 'HAL' but I am glad we kept with it.

Planning LEAS

Before they begin in earnest, Sowley and Arendosh spoke with administrators at other agencies about their needs and what would entice them agree to be clients of NextTech, using LEAS. Administrators at these agencies also had experience with the CIFRS and shared an understanding of the potential benefits, as well as costs to be avoided.

To better shape their system, Sowley and Arendosh conducted a "listening" tour of potential law enforcement agency clients. While it might be assumed that a key selling-point in the design of a law enforcement RMS was security and oversight that was not the case. In fact, when speaking with many administrators, it did not come up in the conversation or, if it did, it was a minor issue. According to Sowley, even when the system was rolled-out and live, after 9/11, security and oversight still was not a primary

theme for their new clients. The primary concerns heard when speaking with agency administrators had mostly to do with the deficiencies of existing RMS, and their collective inability to submit to NIBRS. For many agencies, especially the smaller ones, the ability in the year 2000 to have a CAD system was not critical, whereas a well-functioning RMS was.

What departments were really looking for was a way to use the computer to put the NIBRS reports together, because they could not be compiled manually. This was a big incentive to computerize. It is literally impossible to submit NIBRS reports without the use of a RMS that was designed to report local agency data in NIBRS-compliant ways. For the initial wave of NextTech adopters this, and the access to federal funds, was the reason to adopt a new system: the benefits far outweighed the costs. The second most frequently cited issue concerned the desire to include information technologies in patrol cars.

There were many reasons these police departments wanted network-accessible technology in police cars. They wanted officers out on the road, and not back in the station typing reports. They wanted to give officers the ability to access information from their police cars, which would shorten the information loop. This would free up dispatchers and give officers the ability to query motor vehicle information, wants and warrants, as well as communicate with each other from their automobiles; All of this would allow departments to keep their officers out on the road where they were doing patrol. This comported with an increased emphasis at the time on prevention and deterrence efforts. The commonly held view was that officers were not a deterrent to

crime if they were in the police station, whereas, even if they were doing a report in a car in a shopping center, it could have some deterrent value.

The third most frequently cited theme was that agencies did have an RMS but it was on a DOS, or older, platform. This meant that the employees could neither compile NIBRS reports nor access the state or federal systems from the same computer; other agencies still had no digital RMS at all.

The ability to work efficiently between, or integrate data from, state and federal databases was something that needed to be addressed if the system were to have longevity. It was obvious, even in 1999-2000, that the future involved "smart," or integrated systems. Even if their clients did not think this was critical, Sowley and Arendosh could see integrated systems as a necessity down the road. They felt the same about integrating the CAD function.

In planning the development of LEAS, Sowley and Arendosh had several objectives that the system must achieve, in no particular order:

- *It had to be scalable*. The BPD is the size of and has the call volume of a typical suburban agency; however, they wanted to be capable of selling LEAS to larger agencies whose hourly call for service (CFS) rate was much greater than their own. For example, they wanted to be able to sell LEAS to an urban agency the size of Old Gotham (approximately 450 sworn officers) or to one that was geographically distributed, such as the State Police.
- *It had to work in a Microsoft Windows environment*. This means that a dispatcher could have both the LEAS software as well as the state and federal information systems on a single computer. The AMT system, as well as many similar

localized RMSs used by agencies, was DOS-based. This meant that they had to have separate computing environments that did not integrate (or "talk") in order to work with both local and extra-jurisdictional information. A Windows-based system also meant that an agency could standardize equipment between the different users, and thereby lower costs.

- *It had to accommodate both the local and state coding systems* but allow for reporting and disseminating using the NIBRS standards.
- *It had to be capable of integrating court data* so as to automate the process of keeping case records up-to-date.
- *It had to be designed in such a way as to connect with LEAS installations between multiple jurisdictions*. This would allow, if agencies desired, the ability to share data in real-time (like CIFRS).
- *It could not be dependent on a particular database*. Database technologies have been rapidly changing over the last 10 years and they realized that they had to make a data collection system that was not dependent on a particular database to store the data.

Implementing and rolling-out LEAS

It took almost two years of working nights and weekends to fully develop and test the first generation of LEAS. On January 1st, 2001, LEAS went "live" as *the* system for RMS and CAD for all emergency services in Belleville.The roll-out was surprisingly smooth and worked as designed.

One of the features that won praise from users was the automated way in which LEAS checked records. Suppose an officer wanted to do a records check on an individual. In the past the officer would have had to go through a multi-step process to check the local, state, and federal databases. In contrast, checking the local database the new system would cross-reference various state and federal databases in the background. As Sowley said:

> …when we do the motor vehicle stop and the registrant information is queried, it's also checking the state database for wanted information automatically…it does a lot of maintenance work in the background… checking a much larger sphere of data that the officer doesn't really know about… but it does increase the volume of the data that is being examined.

In addition to streamlining the records-checking process during a field stop, LEAS also was designed to facilitate the booking and processing of an arrested individual. For example, in most agencies the old ink and cardboard system for taking fingerprints has been replaced with a digital hand and fingerprint scanner, known as the Automated Fingerprint Identification System (AFIS). LEAS was designed so that as soon as a suspect's prints are processed by the AFIS machine, they are cross-referenced with the national fingerprint database. In this way a person's true identity, if they are in the system, can be cross-checked; also, the system will automatically let the processing officer know if the individual is wanted on any extra-territorial warrants.

Since 2001 both LEAS and the additional systems used by the BPD have seen exponential growth, in terms of their integration, as well as in features and functions. The

following chapter describes the status of the total DSTs used by the BPD during the time of this study.

Chapter 6: Cross-sectional findings: DSTs in Belleville, 2008-2009

The previous chapter provided a detailed accounting of how the BPD implemented digital surveillance technologies (DSTs) starting in the late 1970s. When those efforts first began they were part of a region-wide distributed network where information was shared between police agencies in several jurisdictions. With the demise of that regional system, the BPD, led by entrepreneurial officers, began to build and manage a series of in-house systems. These systems evolved and grew in both sophistication and scale. These iterations of the system culminated in the mid-nineties with the development of LEAS - a system designed to integrate and centralize all of the endogenous record creation and management functions of the BPD with the exogenous systems (state, federal, and private). Thus, it would serve as both a locus of data generated by the BPD and, over time, a gateway to outside systems.

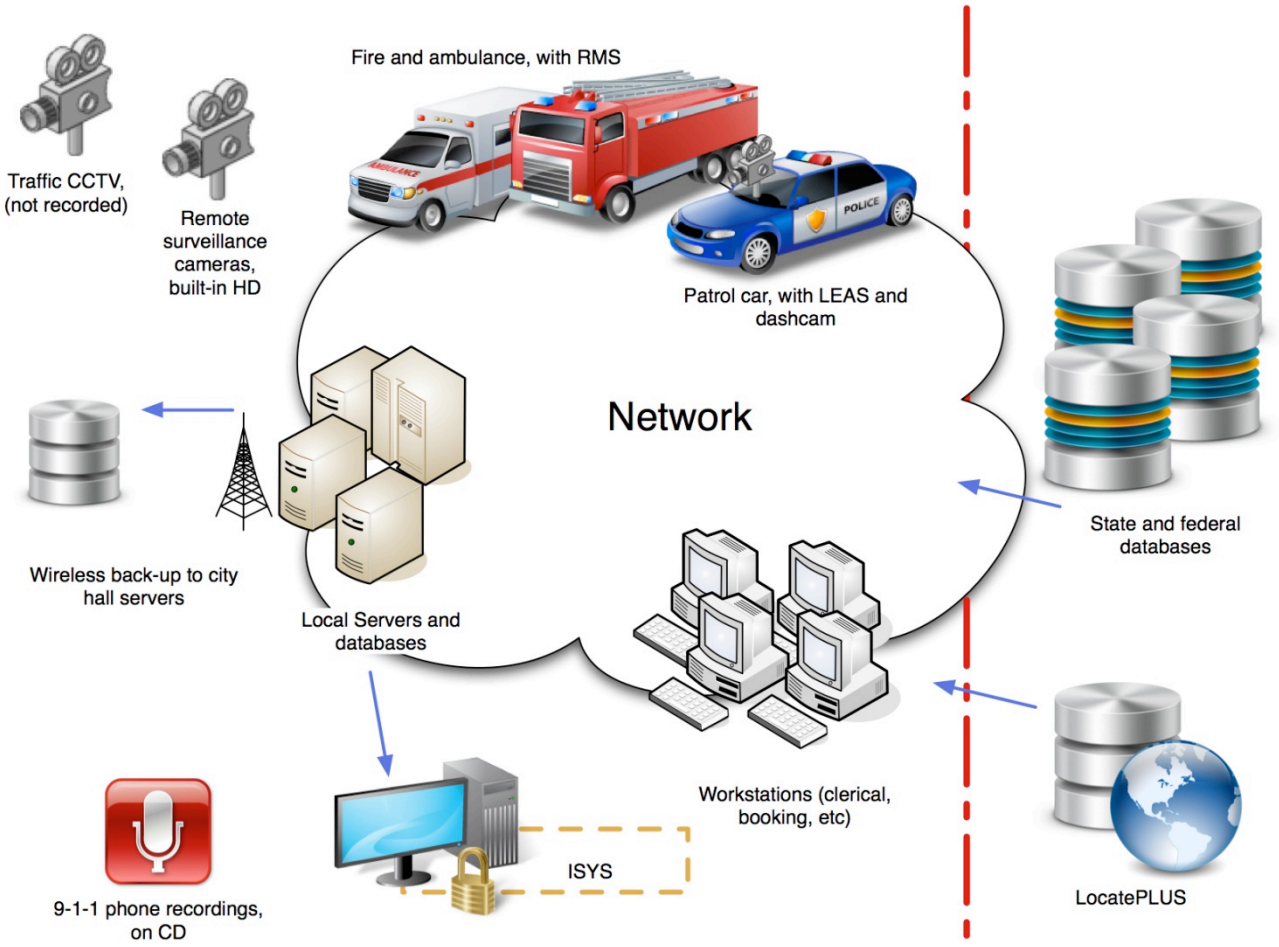
What started out as a labor of love and entrepreneurship eventually evolved into a private business by 1990, NextTech. Since its initial introduction, LEAS has been adopted by over 35 police agencies in the state, including the State Police. To this day Belleville serves as the test site for rolling-out upgrades to LEAS.

This chapter is about the DSTs employed by the BPD during the time of this study. It begins with the central system, LEAS, and also describes the other local, state, federal, and private third-party systems that have been adopted, as well as their mechanisms for administrative control and oversight.

The system of DSTs currently employed by the BPD

The current system of DSTs employed by the BPD includes a comprehensive suite of data acquisition, networking, and management tools. This includes a combination of traditional video surveillance and advanced data analysis tools. The epicenter for the entire distributed DST network is LEAS. Illustration 6, below, shows the complete distributed network. The cloud in the middle represents the LEAS software, which simultaneously provides the capacity for the system to acquire new data by direct input from BPD staff, as well as importing data from state and federal sources.

Illustration 6: Belleville's distributed network of DSTs



This is due to the fact that LEAS has core data collection and management functions and additionally serves as the gatekeeper to networking with most (but not all) of the other systems that make up the total collection of DSTs in Belleville's PD. Other elements directly within the "LEAS cloud" are the local nodes, which include various workstations (some of which are dedicated for particular uses such as 911 calling), computers in the emergency vehicles, surveillance cameras, and locally maintained databases. All of the locally owned data is also backed up to an external server. Radio and 911 call center communications are recorded and are backed-up daily in a CD library which is stored in the 911 call center; however, the individual recorders are not maintained or accessible through LEAS. The BPD employs a textual data mining application, called "ISYS: Desktop" (ISYSS), which imports case data from LEAS; however, it is otherwise a stand-alone and locked workstation. There are three externally maintained database collections that are employed by the BPD. The latest version of LEAS imports data from state and federal sources directly into the LEAS environment, whereas LocatePLUS is a web-delivered information service that is outside of the control of the LEAS environment and is accessible via any internet-connected computer. Each component of the BPD DST network illustrated above is described in greater detail in the following paragraphs.

LEAS

The Law Enforcement Administration System (LEAS) is a comprehensive and interactive computer software system. It is comprehensive because it forms the nucleus of a distributed network that acquires and stores locally created data, networks with several systems, and stores and analyzes data. It is interactive because the system is highly modular and customizable; thus, administrators can turn on and off different features for

individual users based on their role within the organization. LEAS functions fall under two overlapping domains - local data management and access control to external data systems. From the user's perspective, it appears as one giant systemin all but a few instances. In fact, in many respects LEAS functions as a flexible software toolkit designed to facilitate both routine and critical data management functions for emergency service agencies.

The core features and functions in LEAS are grouped into logical "modules" which can be sub-divided into three primary functional areas: Computer-Aided Dispatch (CAD), Records Management System (RMS), and Scheduling and Resource Management (SRM). Each of these functional areas can be used as a stand-alone entity, but all three are designed to work together in an integrated system.

Illustration 7: Presenting… the LEAS modules!

The operational "hub" of LEAS is situated adjoining the 911 call center. This room, located in the center of the police headquarters, looks like a smaller version of NASA's mission control center. The wall facing the operators contains a series of large LCD displays that feature local and national news and weather networks in addition to scenes from the various CCTV's that are primarily used to monitor traffic conditions.

With the exception of the graveyard shift, there are typically three 911 operators on duty at any given time. Each operator has at his command an assortment of communications and computing tools. Each operator workstation includes multiple LCD monitors which contain real-time maps displaying the positioning of all units, as well as access to the various state and local databases.

Illustration 8: Two views of the 9-1-1 call center. The operators at their stations and CCTVs are on the left; an operator workstation is on the right.

Watching the operators work is akin to a improvisational jazz concert. Jill, a 911 operator for nearly twenty years, explains while handling a call: "this job is constantly controlled chaos." Meanwhile, she is switching back and forth between the officers who

are underway, talking with the caller, contacting the EMT unit, checking state records for any warrants or registered firearms, and checking local records for previous incidents involving the caller or location, and intermittently checking a menu to make her lunch order.

Adjacent to the 911 call center is the office of Lieutenant Dan. Dan is responsible for overseeing all of the computer systems and networks. This is an appropriate role for him, as prior to becoming a police officer in the mid-nineties, he was a network IT technician. Dan is a no-nonsense "cop's cop" who also has the cynical "gallows humor" of someone who has been on the job for fifteen years. He takes his job as gate-keeper for the BPD's information systems very seriously. "I have a bottom-line rule that is made clear to *everyone*," he says: "If something bad happens using your account then you own the consequences. It's like my mom used to say: 'You break it, you buy it'". Dan's office is packed with several computers, monitors, and numerous computer manuals. As part of his job he audits and monitors the use of LEAS and the entire BPD DST network. Questions regarding inappropriate use are fielded first by him.[55] Also, it is from Dan's computer that access, permissions, and passwords to all of the LEAS features and access to external systems are tightly controlled.

Illustration 9: Screenshot of the left monitor view of the Dispatcher Screen

[55] This is discussed in further detail below.

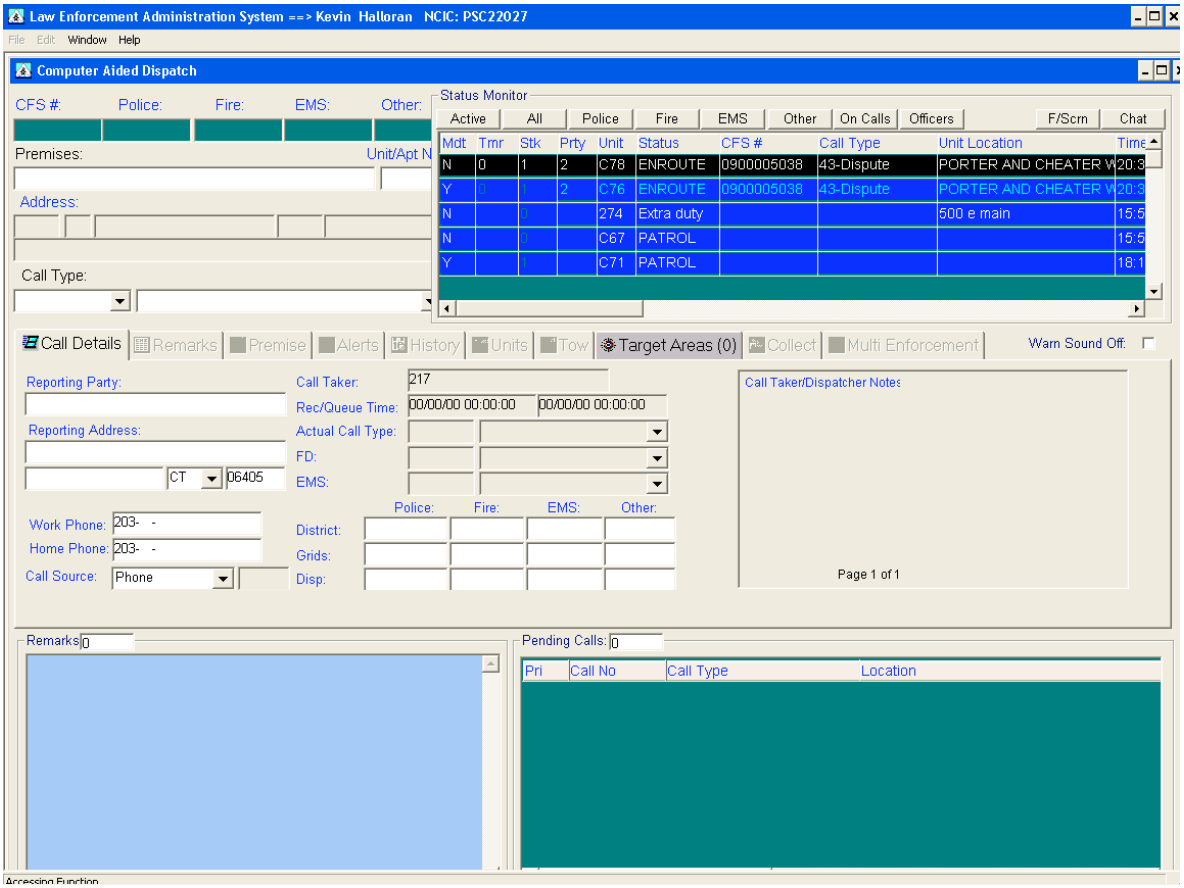

Law Enforcement Administration System ==> Kevin Halloran NCIC: PSC22027
File Edit Window Help
Computer Aided Dispatch
CFS #: Police: Fire: EMS: Other:
Premises: Unit/Apt N
Address:
Call Type:
Status Monitor
Active All Police Fire EMS Other On Calls Officers F/Scrn Chat
Mdt Tmr Stk Prty Unit Status CFS # Call Type Unit Location Time
N 0 1 2 C78 ENROUTE 0900005038 43-Dispute PORTER AND CHEATER W 20:3
Y 2 C76 ENROUTE 0900005038 43-Dispute PORTER AND CHEATER W 20:3
N 274 Extra duty 500 e main 15:5
N C67 PATROL 15:5
Y C71 PATROL 18:1
Call Details Remarks Premise Alerts History Units Tow Target Areas (0) Collect Multi Enforcement
Warn Sound Off:
Reporting Party:
Reporting Address:
CT 06405
Work Phone: 203- -
Home Phone: 203- -
Call Source: Phone
Call Taker: 217
Rec/Queue Time: 00/00/00 00:00:00 00/00/00 00:00:00
Actual Call Type:
FD:
EMS:
Police: Fire: EMS: Other:
District:
Grids:
Disp:
Call Taker/Dispatcher Notes
Page 1 of 1
Remarks 0
Pending Calls: 0
Pri Call No Call Type Location
Accessing Function

Illustration 10: Screenshot of the right monitor view of the Dispatcher Screen

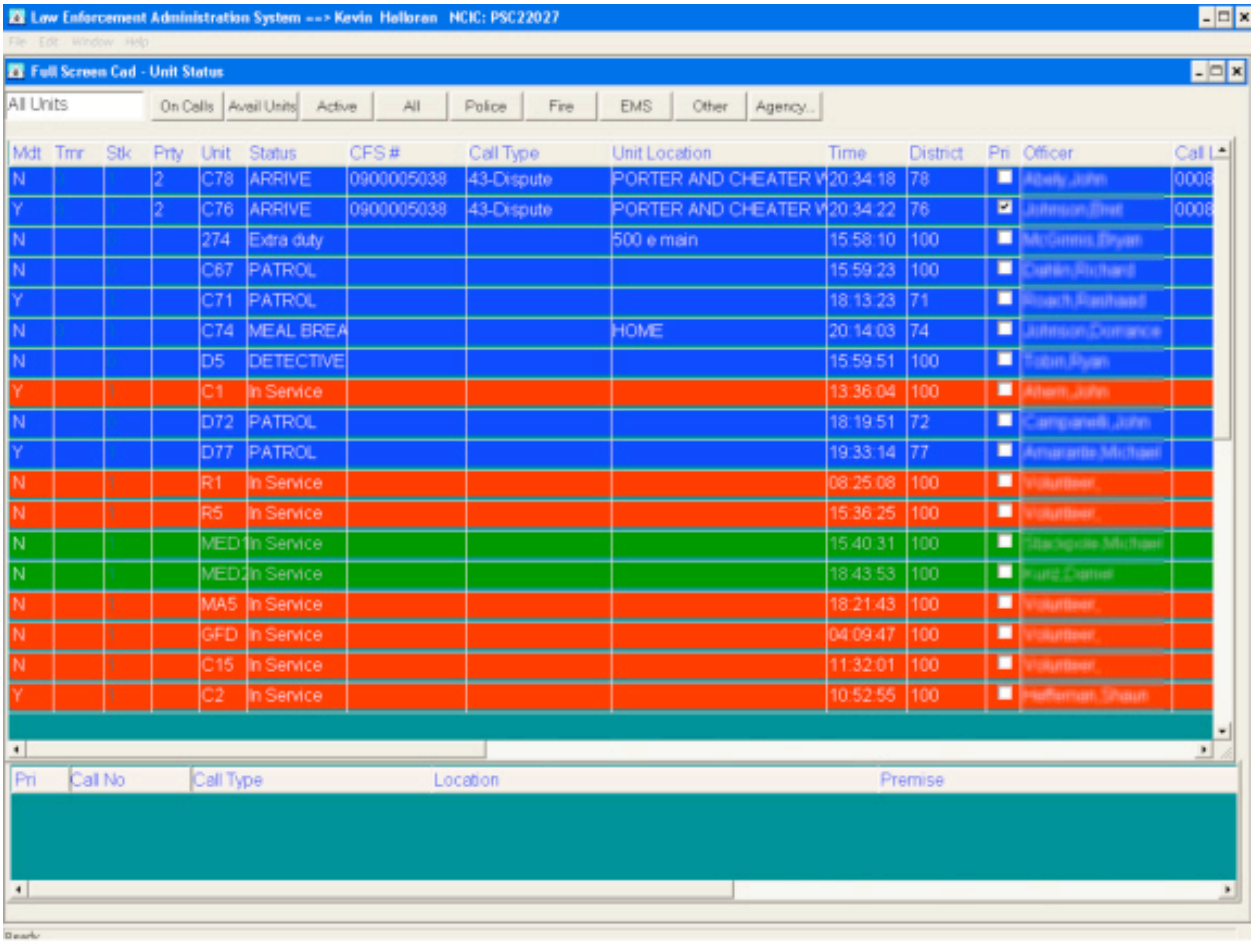
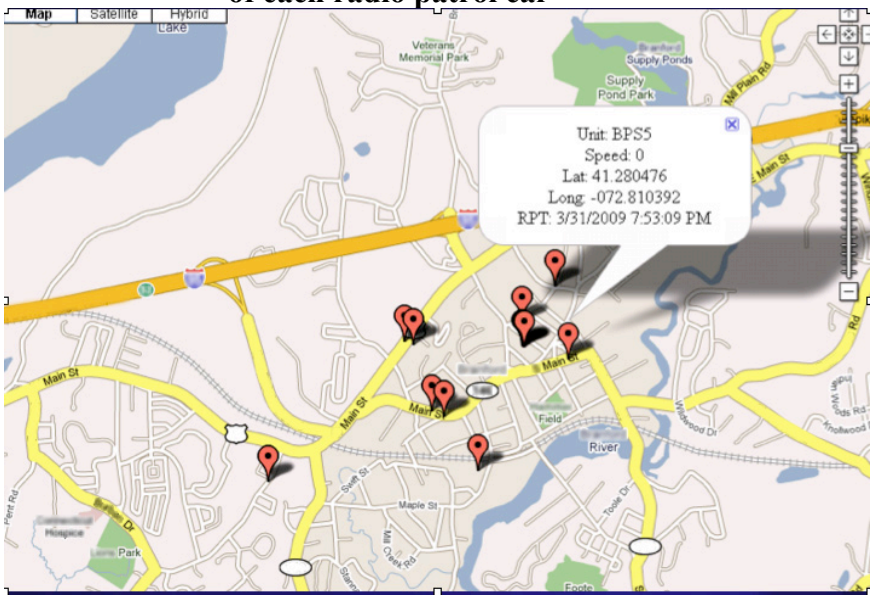


Illustration 12: Detail from dispatch GPS function, pinpoints the location and speed of each radio patrol car



The modules that comprise the core LEAS software suite of features and functions are described below. Many of the modules also contain internal and external data interlinkages. Each module is briefly described below:

- *Alarms.* The Alarms module tracks alarm calls entered in CAD and automatically generates warning letters and bills for false alarms, based on user-defined parameters.
- *Animal Control.* This module allows the agency to track and manage animal records.
- *Arrests*. The Arrests module is where arrestee records are entered and maintained, including arrest, court and booking details, and information such as known aliases, physical descriptors, employment history, photographs, vehicle information, scars, marks and tattoos, and relationships to other individuals.
- *Automatic Vehicle Locator* (AVL). The AVL module displays a map of the town with pinpointed locations of all pending and current calls from the CAD system.
- *Computer-Aided Dispatch* (CAD). CAD is the beginning point of LEAS data collection and management. As calls for service occur, dispatch personnel enter the data which is then automatically assigned system-generated incident numbers.
- *Citations*. The Citations module is used to record citations issued to a person and contains the name, address, and personal descriptor information of the person as well as vehicle information, pertinent information regarding the charge, and the disposition of the citation. This module also provides places to record descriptive information about the person.
- *Department Equipment*. This module is used to record and track department equipment inventory and ordering.

- *Department Notes*. The Department Notes feature serves as an electronic bulletin board. It allows all users to record and view notices of general interest to the agency. For example, users can post requests for shift exchanges or opportunities for traffic duty at construction sites.[56]
- *Field Interview.* The Field Interview module provides a system for officers to record and keep track of persons and/or vehicles noticed during patrol. This module allows records to be kept containing personal descriptors of each subject, vehicle information, and pertinent information regarding the contact.
- *Fire.* The Fire module is an interface that permits the dispatching and management of EMT and Fire information generated in the CAD.
- *Forms.* The Forms module contains state forms that can be printed from the system. This module only provides blank forms for printing. However, pre-filled forms are generated by using other modules (e.g., Arrest).
- *Gun Permits*. Public gun permits are recorded and tracked in this module, including reason for permit, any restrictions, and renewal information.
- *Imaging.* This module allows officers to both capture images of suspects as well as create photo arrays using images from the local database.
- *Incident Reporting.* Incident data is recorded and managed in this module, including the nature of the offense, involved parties, property, vehicles, and narrative reports. Case Incident Reports, warrant applications, and related forms can be automatically

---

[56] Contractors are required to pay off-duty officers to direct traffic when the construction activities potentially impact public safety.

filled in and printed from this module. The Incident Reporting module also has other features that:

  - Checks and corrects for National Incident-Based Reporting System [NIBRS] reporting compliance;
  - Allows managers to assign and manage case activity and resource allocation;
  - Stores related photos and pin-mapping graphics.

- *Jail Management* and *Lockup.* These modules track the current usage of jail facilities as well as the prisoners themselves. They are also used to record the placement of a person in a cell when that person is not an arrestee of the BPD (e.g., if the individual is being held for another agency or if the person has been detained on a warrant and will be turned over to the issuing agency).
- *LEA-Mail.* This is an internal e-mail module; the system is only available within the network and cannot send or receive electronic messages from exogenous sources.
- *Master Business Index* (MBI). The MBI stores relevant data about all businesses in the jurisdiction, such as business names, owners, managers, contact info; however, it also includes all officially recorded information and references, including incidents.
- *Master Name Index* (MNI). The MNI collects data from *all* records management modules about every person recorded in the system. The names of people may be searched in the MNI, allowing officials to view a comprehensive record of the person's association with *any part of the system*. Also, it is designed to allow officials to enter descriptive data about a person who is not captured by any other part of the system.

- *Master Vehicle Index* (MVI). The MVI collects data on vehicles whenever they are entered into any part of the records management system. Officials can view a comprehensive record of all references to the vehicle, including citations, associations with people, and involvement in incidents. This module is sufficiently flexible to allow officials to record vehicle information, thus generating a profile for a vehicle that has not yet been entered in the system which can then be associated with a person or incident.
- *NCIC Log.* All requests (including cancellations) by any users on the local system for data that is held by the state database are recorded with this module.
- *NIBRS Data*. The NIBRS Data module is used to verify the NIBRS data entered into the system each month. It produces error reports to facilitate correction of errors and generates the final report that is submitted to the state.
- *Outside Work.* This module is used to set up, track, and maintain private duty work, including company information, private duty job details, and personnel assigned to private duty jobs. There are various circumstances where private businesses are required to pay the BPD for services. One example, is directing traffic for construction sites. These jobs, or 'outside work', are offered to off-duty officers as extra pay. The BPD pays the officers directly and bills the client; however, time accrued for 'outside work' does not count toward the officers pension.
- *Pawned Property*. This module maintains a record of pawned property. Licensed pawn brokers are required by law to provide police with updated records. When a description of a pawned item is entered, LEAS automatically displays a list of stolen items of a similar description and the corresponding incident number.

- *Personnel.* This module is where all agency personnel are entered into LEAS. This module interfaces with many other LEAS features, including the CAD and System Access modules and the Scheduling modules.
- *Property and evidence.* This module tracks and manages impounded property and evidence, including chain of custody.
- *Registration.* This module allows the agency to record registrations of property by members of the public, such as bicycles.
- *Reports.* This module allows administrators to create reports from data held by the system.
- *Shift Setup, Assignments, and Bids*. These modules allow administrators to manage the details of scheduling, including shifts, rotations, patrol areas, and ranks, in order to build a complete shift schedule. They also allow officers to put in requests for shifts and allow managers to view run-rates and shift costs.
- *Target Areas*. This module allows administrators to assign locations that need extra attention by patrols. A target area is any single location (by address or premise name) or area (by street address range) that is considered for extra patrol. Examples include vacant houses and crime "hot spots."
- *Training.* The Training module manages department training information, including setting up course dates, locations, and times, scheduling personnel for training courses, and recording scores and certification of personnel.
- *Vehicle Maintenance*. This module allows the agency to maintain a complete profile of agency vehicles, including maintenance records and gas logs.

- *Warrants*. The Warrants module maintains a record of warrants applied for by the BPD, tracks the disposition of each warrant, and allows officials to create and print an Arrest Warrant Application form. This module also allows entry of various details about a wanted person, including physical descriptors, vehicle information, known aliases, and relationships to other individuals.

Video surveillance

The BPD has three separate systems for video surveillance. The most frequently used system consists of a series of fixed-location cameras that monitor roadways and intersections where crashes are most prevalent. This system is monitored by the 911 operators via a LCD monitor that is wall-mounted in the telecommunications center and is directly visible as they work; however, footage from these cameras is not recorded.

Recently the BPD obtained a second video surveillance system. These are remote cameras that can be discreetly and remotely mounted. This technology uses a digital hard-drive; thus, this allows the captured video imagery to be digitally recorded. The remote cameras are primarily used to monitor a particular person or location as part of an investigation or crime suppression ("hot spot") program.

Lastly, each radio patrol car is equipped with a video "dash cam." This is a system that records both video and sound, and is used to record what happens during an incident. Whenever the emergency lights are turned on the video camera is automatically engaged and stays engaged until the lights are turned off. An officer can independently start and stop the video recording if the lights are not engaged; however, once they are on, the video can only be turned off when the lights are switched off.

Illustration 13: Inside the Belleville patrol cars, detail of dash cam mounted on rearview mirror (left) and the LEAS computer terminal (right)

The researcher asked several officers about what they thought of the dash cams, presuming that there would be some kind of unhappiness with being "watched" while they work. One officer remarked, "We love 'em… do you realize how many times some jackass tries to jam us up for doing our job?" This sentiment was a constant refrain.

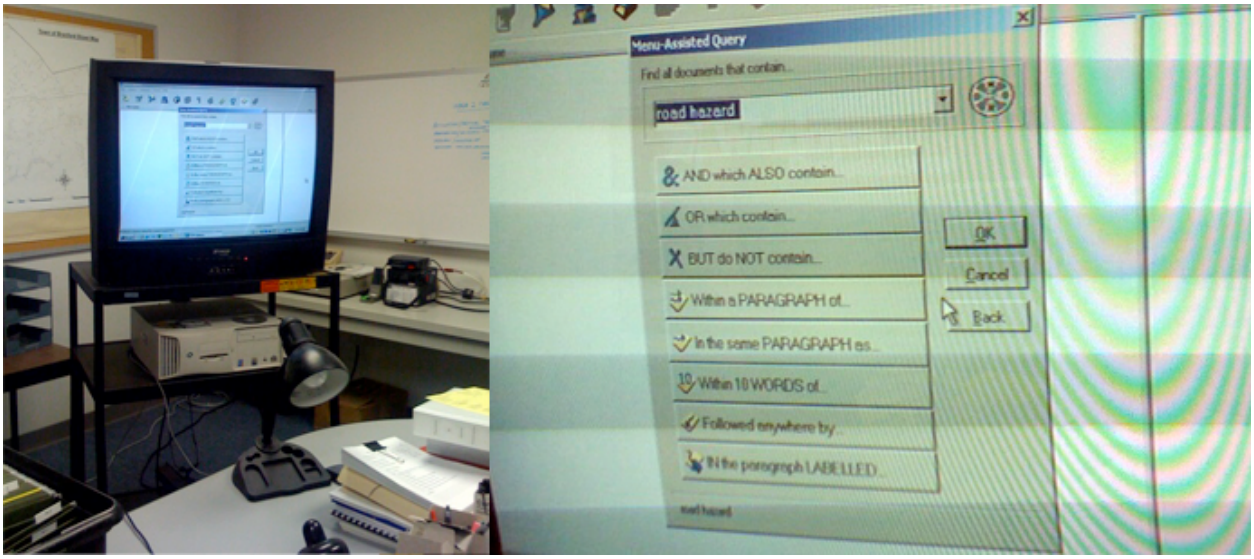
The data is stored on a SD card, which is housed in a tamper-proof container and is automatically and wirelessly backed up when a radio patrol car is brought into the garage between shifts.

During the final stages of the research, the BPD began the planning stages of testing a video and sound recording device that is worn by an officer on the lapel of his uniform. Another technology under consideration is a video and sound capture technology which is housed in a flashlight.

ISYS Search Software

ISYS is a text- (or semantic-) based data mining analysis tool that is employed by the BPD. ISYS was created and is distributed by an Australian software firm. ISYS simultaneously analyzes text-based data held by the BPD across different databases. It employs an analytic approach based on a 'fuzzy logic' scheme: as such, it searches for approximate patterns and relations in the data. What makes this different from the existing technologies is the ability to search within the descriptive case data as well as the tabular case data, whereas existing search functions in LEAS are limited to tabular data. "When we first turned it on" one detective explained, "we had just investigated a stolen car incident and I entered the details of that case into the search field… It was able to identify connections with the six other cases - the oldest being almost 18 months earlier. This led to the break-up of a ring of car thieves that were operating in several jurisdictions." Unlike the LEAS system, ISYS is a segregated system that exists on one computer in a room otherwise dedicated to emergency management. It is not a room that is ordinarily trafficked. ISYS and the workstation that it is on is only intended to be used by officers who are conducting investigations.

Illustration 14: ISYS workstation and detailed view of main search function



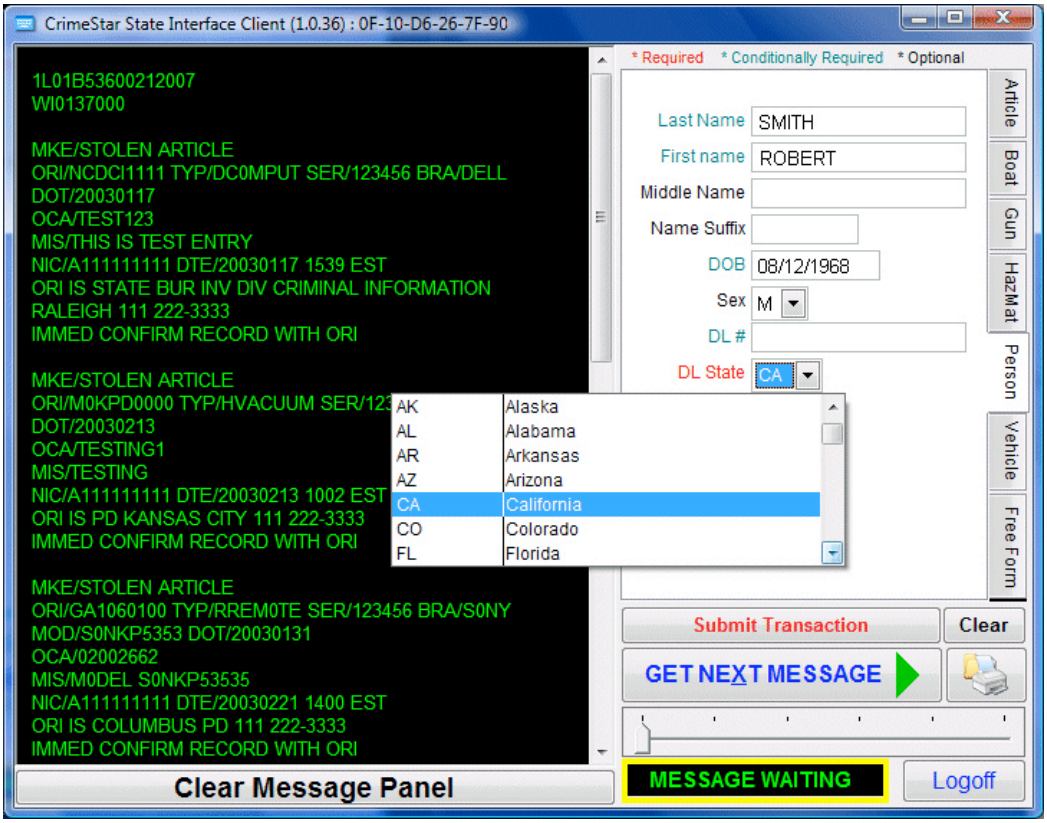
State and federal information systems

There is a standard and comprehensive suite of databases that are offered to local law enforcement and maintained by either state or federal agencies. The entire list and descriptions of the databases is contained in a 3 inch binder. These exogenous systems are accessible by users of the BPD system through LEAS. In this way, information can be accessed and connected to local case files, as warranted. Also, this allows the users to stay within one computing "environment" while assembling the collection of data that might be needed on a particular case.

The state's databases include DMV records (with ID photos), warrants, prison and probation records, gun permits, criminal history, AFIS, and addresses.

Federal databases include that national registries for fingerprint identification (NAFIS), real-time crime and stolen property data (NCIC), emergency management/homeland security (NLETS), as well as inter-state telecommunications between agencies (the latter used to be done with teletypes).

Illustration 15: Detailed view of the NCIC database interface



LocatePLUS

LocatePLUS is a powerful tool for conducting investigations and background searches. It is a web-based service that provides an extensive and comprehensive data suite that is culled from public and private databases throughout the country. The system's power is due to a flexible search interface that contextualizes data related to all of the search subjects/data points that are contained in the database. Therefore, it can be used to assess the potential social networks and relations between search subjects and their neighbors. In this way, each data-point can be used to connect and interlink people, places, and things.

LocatePLUS' search interface permits investigators to search by eight broad categories, which are explained below:

- *Person.* This category makes it possible to search by a person's name, social security number, current address, aliases, and common residence; it can also identify up to 30 years of previous addresses, identify possible relatives, and find neighbors' names and addresses
- *Phone.* Investigators can conduct reverse searches on unlisted and unpublished phone numbers;[57] moreover, they can also conduct reverse searches of cellular and fax numbers, as well as identify which firm is the cellular carrier for a particular number. Investigators can also determine historical data pertaining to cellular numbers, owners, and usage patterns.
- *Motor vehicle records.* This search function permits the investigator to enter full or partial plate and VIN number of a vehicle; Furthermore, the system can also search for current and prior automobiles that were owned by a particular person. Additional information can be obtained about an individual's driver history and driver's license data.
- *Court records.* This is a comprehensive database that includes a variety of criminal and civil categories, such as court cases and numbers, legal actions, civil records (including bankruptcies and divorce records), liens, plaintiffs, and incarcerations.
- *Criminal records.* These records include felony and misdemeanor charges, adjudications, and sex offender registry data.

---

[57] According to the LocatePlus documentation their database contains about 95% of all unlisted and unpublished numbers nationwide.

- *Property.* This permits the investigator to search by address, P.O. box, city, and zip code.
- *Vessels.* Information pertaining to boats and watercraft (based on vessel name, call sign, or owner) is also available to investigators.
- *Corporation records.* This final search area contains detailed information about both public and private firms, including historical data.

Local data repositories and back-ups

The internal system is hosted on a Windows Enterprise Server with over 10 terabytes of disc space. Within the server environment there are several partitions, and each has a redundant local back-up. Additionally, there is an offsite back-up in the Belleville City Hall, which is connected to the BPD via a dedicated wireless data transmitter. The various partitions serve different functions. For example, one is used to host the LEAS code; another, running SQL, contains all of the tabular data collected by LEAS; a third partition holds the photos collected by the BPD; the 911 call center has its own partition to store critical incident data; and ISYS has a system where it pulls information from the other databases as needed but it does not upload information into the other databases. The "dash cam" video files are stored on a system that is independent from the others. The audio recording from the 911 calls are digitized and transferred to CDs. The library of CDs is stored in the 911 facility.

Illustration 16: View of the database room (left) and detailed view of the primary LEAS data server (right)

Applications of the DST system

As evidenced by the preceding description, there are many reasons why information is captured and managed by the entire collection of the DSTs employed by the BPD; however, not all of them are used with equal frequency. For example, not every incident in the system leads to an arrest and jailing of a suspect. A review of the BPD's logs shows that the most common scenarios whereby information is either captured or "managed" in some way are dispatching and resource management (on a call), processing suspects, case management (including evidence and form completion), DMV and identity checks, and administrative tasks.

The following three cases provide an illustration of the variety of ways that DSTs are employed to respond to and solve crimes. The first is a composite "typical" case that is illustrative of the volume of data (both mundane and critical) that is collected when responding

to “everyday” calls for service. The second case, a real bank robbery, illustrates the reality that, despite the many ways that DSTs have become indispensable to modern policing, human relations are still a critical cog in the machine. The third, and also real, case is meant to illustrate how the very technologies used to bring efficiency to crime prevention can be used to identify and root-out official corruption.

Case 1: A typical call for service

During the time of this study the researcher spent over 200 hours directly observing 911 operators, police officers, and administrative and clerical staff. During the course of this inquiry the researcher witnessed police conducting all aspects of police operations- from providing public safety at the scene of auto accidents to booking arrestees. The following is a composite, or as Gerring (2007) calls it, “synthetic” case culled from many observations, stitched together to tell a single coherent story in order to illustrate how and what data is typically captured and observed by the system (and the users of that system) from a typical call for service. As Gerring (2007) argues, following upon Abadie and Gardeazabal (2003), the synthetic case inclusive of the various dimensions under study provides a baseline when conducting inductive case study research.

It is 9 o’clock on a Saturday evening and atypically warm for January. So far, the shift has been uneventful, when a concerned citizen calls to report suspicious activity in a car sitting in front of 1313 Mockingbird Lane. The dispatcher immediately sets to work. The call coming in immediately generates a unique call for service (CFS) number in LEAS. The operator enters data about the CFS (two males have been sitting in a car in front of the house for three hours); meanwhile, in the background LEAS is automatically collecting data about the caller. The concerned citizen is calling from a land-line, which allows for an instant trace. The operator

enters the caller's name and information which, may or may not be, the same as the name on the account. Both pieces of data are maintained on record. The operator's screen is illuminated with information pertaining to the individual on the phone, her local criminal or victimization history, and any service calls pertaining to the residence she is calling from. This information about the caller will stay with the electronic file. In this particular case, it appears that the caller doesn't have a history connected with the address where the suspicious activity is being reported.

The operator enters the data provided. The location of the reported activity, a rental house in a low-income neighborhood, has a history of service calls - mostly for loud parties. It is also on a watch list for suspected drug activity. The system evaluates the type of call, the residence location, and the location and utilization of current resources (patrols), and recommends the dispatch of Officer Smith.

At 9:10p.m. Officer Smith is dispatched to the call on Mockingbird Lane. All of the information pertaining to the call is instantly transmitted to the data screen in his patrol car; meanwhile, the operator is providing Officer Smith with critical details over the as he radio drives to the scene.

By 9:25, Officer Smith has arrived at the street. He slowly turns down the street and observes the suspicious car, a Red Honda Civic, about 45 yards ahead on the right. At this point he goes "dark" (no head lights) and drives toward the Civic, stopping about 20 feet behind it. In the reflection from the streetlamp he can make out the license plate. He punches the number into his computer and while awaiting the response from the state DMV, he "lights up" the suspect vehicle with his strobe and headlights, which also initiates the "dash cam." Meanwhile, the computer lets him know that the Civic is owned by an Eric Zepinah of Old Gotham, who has a felony record with the state for possession and sale of narcotics.

Officer Smith calls for back-up, gets out from his vehicle, and approaches the suspect car cautiously. He finds two young ladies who are a bit surprised by his appearance. He asks for their license and registration. The driver, Giovanna, provides her license but does not have the registration. Her passenger, Angela, claims to not be able to find her license. Meanwhile the back-up officer, Webb, has arrived on the scene. Smith asks the pair how long they have been sitting there, and they claim to have arrived only moments before. As the pair is being questioned Webb shines his flashlight into car, and notices what appears to be a crack pipe sticking out of Angela's jacket pocket. He asks her to step out of the car. As she is getting out she accidentally drops a baggie of crack rocks. Angela is placed under arrest for criminal possession. Giovanna, who claims to know nothing about the crack, is also placed under arrest.

Angela and Giovanna are both read their rights and put in the back of the police cars, and the two are taken into custody while their car is impounded.

Around 10 p.m. they are brought into the booking room, in the lower level of the BPD. Both women are processed, or "booked." The entire process is caught on surveillance cameras. This process involves a standard set of questions about the individual's identification. If the person is already in the local or state system then the process is very quick. In Giovanna's case, Smith enters her Social Security number and it immediately gives him access to her state and local files. She has been arrested before on minor charges, and the computer also shows her DMV photo and it matches her appearance. All that is left at this point is to digitally take her fingerprints and cross-reference those with the state and federal fingerprint systems. They all match, and she is then put in a cell to await arraignment the next day.

Illustration 17: Booking workstation and booking cell (through the bars)[58]

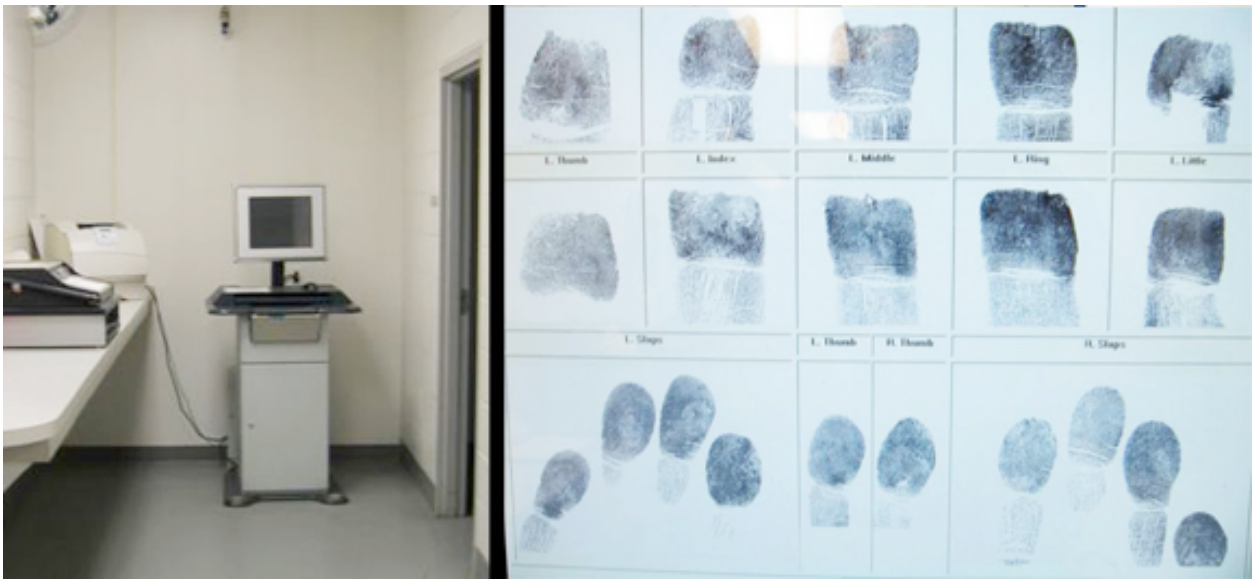
Angela's story is a little different. She has not provided ID to verify the name she gave- "Angela Shoeman". Officer Smith can't find any entry in the state system for anyone named "Angela Shoeman;" "Angela" explains that she has just moved from Ohio and doesn't have a record. Smith enters all the data that Angela provides, photographs her, and then leads her to the digital fingerprinting machine - which is where her story begins to fall apart.

Angela attempts to move her fingers while the machine is scanning; however, the machine alerts the officer and it will not process the fingerprints until it is able to obtain a "good" scan.

---

[58] To the right of the camera is a sign that reads: "Remember, If an arrestee has any tattoos, take pictures of the tattoos! Very important for future investigations".

Illustration 18: AFIS workstation (left) and screenshot of scanned prints (right)



Within minutes the scans are complete and the machine alerts the officer that "Angela Shoeman" is actually Angie Shop. The computer has cross-referenced her fingerprint data, alerted Smith, and brought up her photo and identification data; moreover, Angie Shop has an extensive criminal background in Ohio which includes felony evasion and felony narcotics possession with intent to distribute. There are currently two bench warrants out for her arrest in Springfield, her hometown, and Shelbyville - both for "failure to appear" on misdemeanor charges.

Officer Smith locks Angie up and returns to the computer to re-associate her data with this arrest. He also includes her real identifying information along with the false information that she provided, and all of the charges, which now include a charge of misdemeanor identity theft.

After the processing of the individuals is complete, Smith must then process the evidence. This is done by taking the evidence and the valuables and logging their entry into the

system. They are placed in paper bags which are sealed with a sticker that has a bar code, which is generated by LEAS. This ties the evidence to the specific case. The evidence is then put into a special locker that, once closed, can only be opened from the Evidence Room, which is on the other side of the outer door of the locker. Only the Evidence Officer and two other executive officers can access the Evidence Room.

Illustration 19: The workstation for logging-in evidence (left) and the evidence lockers (right); once evidence is secured in the locker only select administrators have the ability to open the door.

After the offender and the evidence are secured, the next step is for the officer to dictate the tabular and narrative data into an audio recording device. The dictations follow a particular sequential script. The recording is then submitted into a queue for the clerical staff to process.

The clerical staff cross-references the narrative with the data that has been entered into LEAS, and they also ensure that the narrative and other data is grammatically correct. Discrepancies that are substantive to the case are brought to the attention of a supervisor: finding

none, the clerk returns the completed form to the officer for his signature. This process is done in lieu of a hand-written form, and has been in place for over 40 years.

When the clerks have completed this process and the narrative and tabular data has been cross-checked and validated, the state and county forms can now be efficiently generated, signed-off, and transmitted to the appropriate parties (courts, prosecutor's office, etc).

Case 2: Bank robbery

During the summer of 2008 there was a bank robbery in Belleville. Two armed gunman entered a bank and demanded cash. This could not have been their first bank job. They chose the only bank in town that does not have Plexiglas between the tellers and patrons, as well as being the easiest to escape from. When they entered, one gunman jumped on top of the counter ordering everyone to the ground while his partner took cash from the tellers. Within five minutes they were gone, having stolen over $100,000 from the bank. They got away but they left behind three pieces of evidence that would eventually lead to their being caught and convicted. The first was a partial fingerprint where the gunman put his hand to steady himself as he jumped on the counter. Secondly, the video camera caught a partial glimpse of the other gunman's mostly-covered face - which revealed a very stylized pair of glasses. Lastly, they ditched their getaway car on a remote one-way street.

The following week, while on patrol at 3a.m., a young officer observed suspicious activity near where the car had been dropped, and he stopped to inquire. When the driver was asked to show his ID he made some comments about "going to FoxWoods to gamble," and that he was lost. Given the street's out of the way location, and the time of night, the story that the citizen gave did not "add-up." His suspicious activity and location was not, in of itself, illegal. However, this chance encounter, the cooperation of public and private actors, and the tenacity of

the detective assigned to the case, Detective Picasso, ultimately lead to the solving of over 5 bank robberies spread out around the state.

The young patrol officer, Jones, reported to Picasso the next day what had occurred, and provided the information from the initial check into the suspect's background. Further inquiries allowed Picasso the ability to build a dossier of the suspect and his behaviors, including the trip to FoxWoods. The casino provided the detective a detailed accounting of the suspect's transactions, which totaled more than $250,000 in the previous two years. The suspect was a member of the Casino's loyalty program; thus, every time he sat a table he swiped his card for points. However, that also meant the times, dates, and even the precise locations of his gambling activity were known. The suspect had been to the Casino since the robbery and had gambled in excess of $20,000; casino cameras, moreover, photographed him with a friend who resembled the other suspect who was partially visible in the bank robbery video.

With this evidence in hand, Picasso called in a favor at the Old Gotham Police Department. Could he use their face recognition software on the bank robbery and casino footage? The results were indeterminate; however, the local files at the Old Gotham Police Department had additional information about the suspect and his known accomplices, which eventually lead to the identification of the second man. From there, Picasso enlisted the help of the FBI, whose access to IRS records was most helpful. The suspect's tax history showed that he had not earned more than $5,000 a year for the previous two years - which, given his gambling habits, was at least curious.

One of the problems that Picasso faced was tracking down where the suspects lived. Their last known address was a jail. Their official addresses on their state I.D. were long dormant. From their FoxWoods account, Picasso was able to obtain a cellular phone number, for

which he was granted a warrant to get the records from the carrier. Most of the calls were made to and from disposable phones, with one exception: there were a lot of calls to and from a woman who, it was later discovered, was the suspect's girlfriend.

Picasso observed that the pattern of gambling was in clusters. He plotted backward from the occurrences of gambling and made a discovery. Within a week prior to each cluster of gambling activity, there was a bank robbery reported somewhere in the state. More importantly, those robberies had similar M.O.'s to the robbery in Belleville. Picasso contacted his colleagues at the different agencies in order to obtain and share information. The data collected began to mount against the suspects.

The decision was made not to arrest the suspects, but to monitor them in an attempt to catch them in their next heist. This decision was made because the evidence, while more than suspicious, was too fragmented to make a case in any one of the jurisdictions where the previous bank robberies had occurred. These were all cold cases at this point.

Picasso called in another favor. He had a friend who worked at the Ackerville Police Department, and Picasso had heard that Fairfield had a GPS tracking device that they could put on a suspect's automobile which could then be tracked through the internet. For several weeks, they tracked the suspects and actively surveilled them using this approach; however, there came a point where the signal did not work as expected. During that time, there was another bank robbery that followed the same M.O. as the previous heists. Also, the car that was identified as the getaway car fit the description of the car that they had been tracking. Within a day or so the getaway car was located with the GPS device still attached. Picasso, along with the local police in the jurisdiction where the robbery took place, set up a stake-out on that car hoping, as in the previous case, that the suspects might return. The officers employed surveillance cameras to

video the car. After a few days, the suspects returned to retrieve their car. They could be seen in the surveillance video slowly driving up and down the street, observing the car and the environment… in the next scene they are seen getting arrested.

The suspects were charged with bank robbery in the most recent case; however, they were given an opportunity to plead guilty to a charge that would subsume punishment for the other bank robberies. One suspect decided to turn state's witness, while the other claimed innocence. At the time of this writing the trial is still pending.

Case 3:An atypical case

The DSTs of the BPD are not only useful for surveilling potential citizens who are offenders, but also for monitoring violations of protocols for using the system. These violations, committed by officers or civilian personnel, are frequently a matter of oversight or innocent error. Such is the case when an officer errantly puts the wrong sticker on the wrong evidence bag. A problem, yes, but not necessarily one of willful misconduct. However, the detailed accounting that systems like LEAS provide about who accessed what module to conduct which action at what time can help reveal patterns of purposeful and willful official misconduct.

An illustrative case involved a high-ranking previous BPD executive officer who was induced to resign in 2006. In that case the officer had taken a loan to purchase an investment property. He was telling his colleagues that he was getting ready to retire and that owning properties seemed like a good investment for his future. Unbeknownst to his colleagues, he was logging in to LEAS and checking the state records of potential renters of his property. To do this he had to log in and connect those searches to a specific case. He connected his searches to a dormant case that had already been adjudicated.

The senior officer misjudged the odds of getting caught using the state databases for personal purposes. Within a few weeks state auditors had shown-up to investigate. Their tip-off was a search being done by an executive officer, which was unusual. The previous time the executive's user ID had been used to look into the state system was five years earlier. Suddenly, his user ID was very active. In the end the state and city negotiated an outcome. The executive officer would agree to retire and the BPD would be able to keep its status as an 'in compliance' user of the state system.

The details surrounding the former executive officer's departure were only revealed at the end of this study. However, it casts a new light on a statement the current BPD Chief made early in this study when this researcher asked the Chief to demonstrate specific features of LEAS: "I can't do that, I'm only the Chief!" What at first appeared to be a joke turned out to be a commentary about how he and all of the other employees have their access strictly limited to only those features of the system that relate to performing their specific jobs.

Oversight mechanisms of the DSTs

The mechanisms for oversight of DSTs employed by and local law enforcement agency fall under two broad categories - human and automated - although there is much overlap between them, as well as interdependencies. Also, the job of oversight is a shared responsibility between the local jurisdiction, the BPD, and the external state and federal agencies.

Endogenous oversight mechanisms

The BPD has a variety of mechanisms that serve as deterrents to bad actors, provide guidance for avoiding of mishaps, and assist administrators in scrutinizing the uses (and users) of the system.

"We take the attitude that one asks for permission and not forgiveness," explained the Chief. "Yeah," adds Lieutenant Dan, "the last thing I want is to be professionally embarrassed by one of my guys paving the road to hell with his good intentions." Thus, when the Chief and his executive officers re-drafted the BPD's "Standing Orders" in 2006, they updated the training protocols and requirements with respect to the use the DSTs. The current Standing Orders include extremely specific language about the obligations and duties of officers as they relate to the critical daily functions of the agency and its various DSTs. For example, employees can be formally reprimanded or brought up on departmental charges for leaving a terminal without logging out. The researcher witnessed several occasions when the ire of Lieutenant Dan was brought to bear on an officer for this lapse. Also, passwords are changed monthly to enhance security.

Each employee is required to pass an annual re-certification on the use and protocols of his local DSTs. These protocols cover a wide range of critical data acquisition and management areas, such as:

- The collection, dissemination, and retention of juvenile records. This includes an explicit method for distinguishing juvenile records; the handling of unique identifiers (fingerprints, photographs); additional security ascribed to that data in the system; and, when necessary, a means for disposition and expunction.

- The management and control over the type of data that is obtained using third-party information providers, such as LocatePLUS.com.
- Guidelines and procedures for logging and tracking evidence from crimes and crime scenes, using the RMS.
- Guidelines establishing privacy and security precautions with respect to digital data that is held by the BPD, including rules establishing who has access and control to certain data (and under what circumstances it can be accessed), as well as criteria and procedures for the release of local records.

As part of the BPD's standard training regimen, employees are shown all of the ways in which their activities are monitored and delimited on the system. The explicit purpose of this is to serve as a deterrent for unwanted behavior, and to instill a culture of respect for the rules and expectations pertaining to the DSTs

If the stated rules and protocols are, at the most simplistic and aggregate level, the first line of defense, then the second line is *direct* human oversight. At the BPD this occurs in several ways. First, certain systems (like ISYS) are contained in spaces which are not normally trafficked but are highly visible. In the case of ISYS, it is located in the Emergency Management Center, and is displayed on a specific work station that has attached to it a large (42-inch) LCD monitor. There is no way a person can be either in the room or using ISYS without being observed. Secondly, case data is reviewed and crosschecked against official records and the dictations made by officers. Each time a user logs in anywhere in the system, the login, logout, applications, and systems features used are recorded using computerized logs (see below). The

logs for both the locally maintained and third-party/exogenous systems are audited on a weekly or bi-weekly basis, depending on the specific system.[59]

The BPD employs a cross-section of automated and mechanical tools for controlling, observing, and delimiting access to and use of DSTs. While some of these require a human element, nonetheless, they are considered the micro line of defense because they are ultimately embedded within the functions of the DSTs themselves.

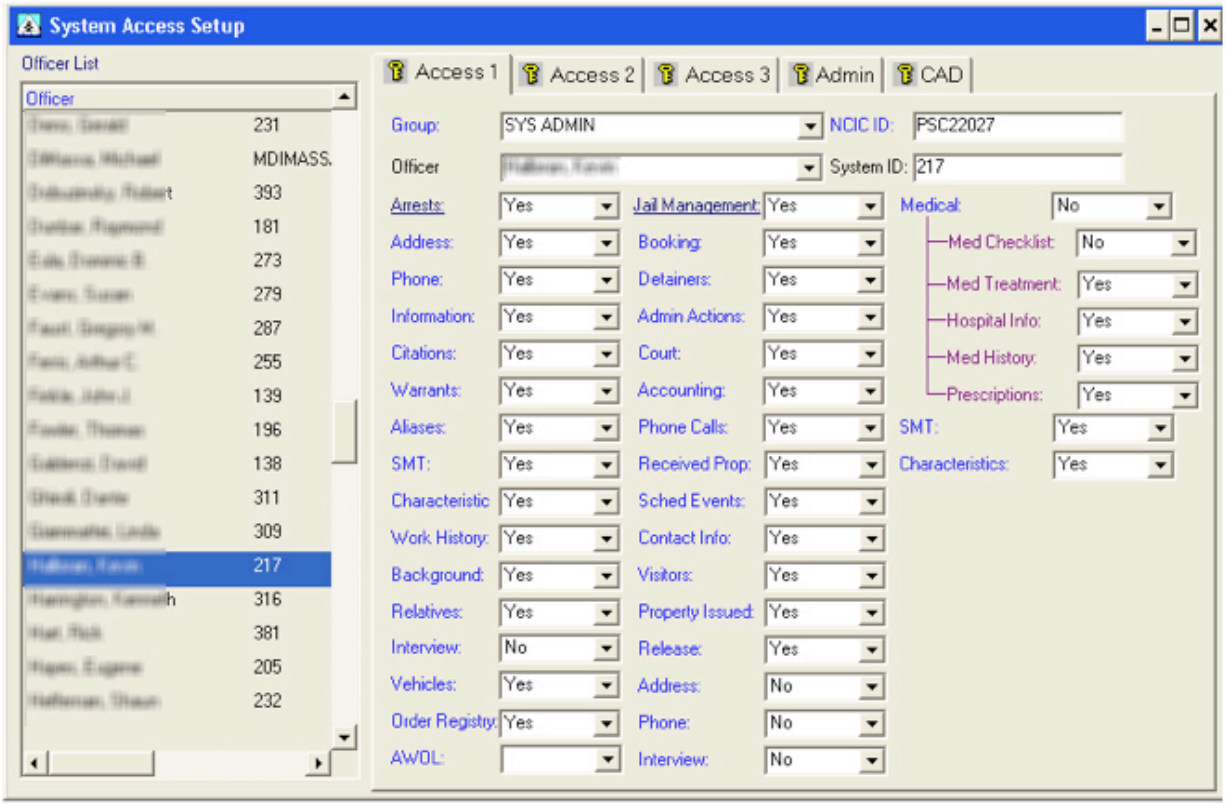
There are two mechanical features that are especially "human" centric. First, every DST application and system is coordinated through a centralized control panel (pictured below). Everything, from an individual's password to the specific features he can access are logged here. The system administrator is the only person who can access this control function.[60] He works

---

[59] For example, the logs from LocatePLUS are only reviewed bi-weekly by the head of the Detective Division because that service is less frequently used than most others, whereas the LEAS logs are reviewed weekly by administrators.

[60] However, they have a contingency mechanism in case of unforeseen circumstances where the system administrator, Lieutenant Dan, cannot be available.

Illustration 19: System access panel



with a set of pre-determined “access profiles”. Thus, if a new person is hired or a person is shifted from one role to another, changing their status in the system will then automatically change all permissions and accesses relevant to that new role. For example, if someone was shifted from detective back to patrol, then the administrator would simply make that status change in the access panel and it would automatically de-authorize the officer from the “detective only” parts of the system. However, the system is sufficiently flexible so that the administrator can customize a person’s access level. For example, the Community Officer is technically a “patrolman,” but his role requires him to have access to certain data management features that are specific to his job.

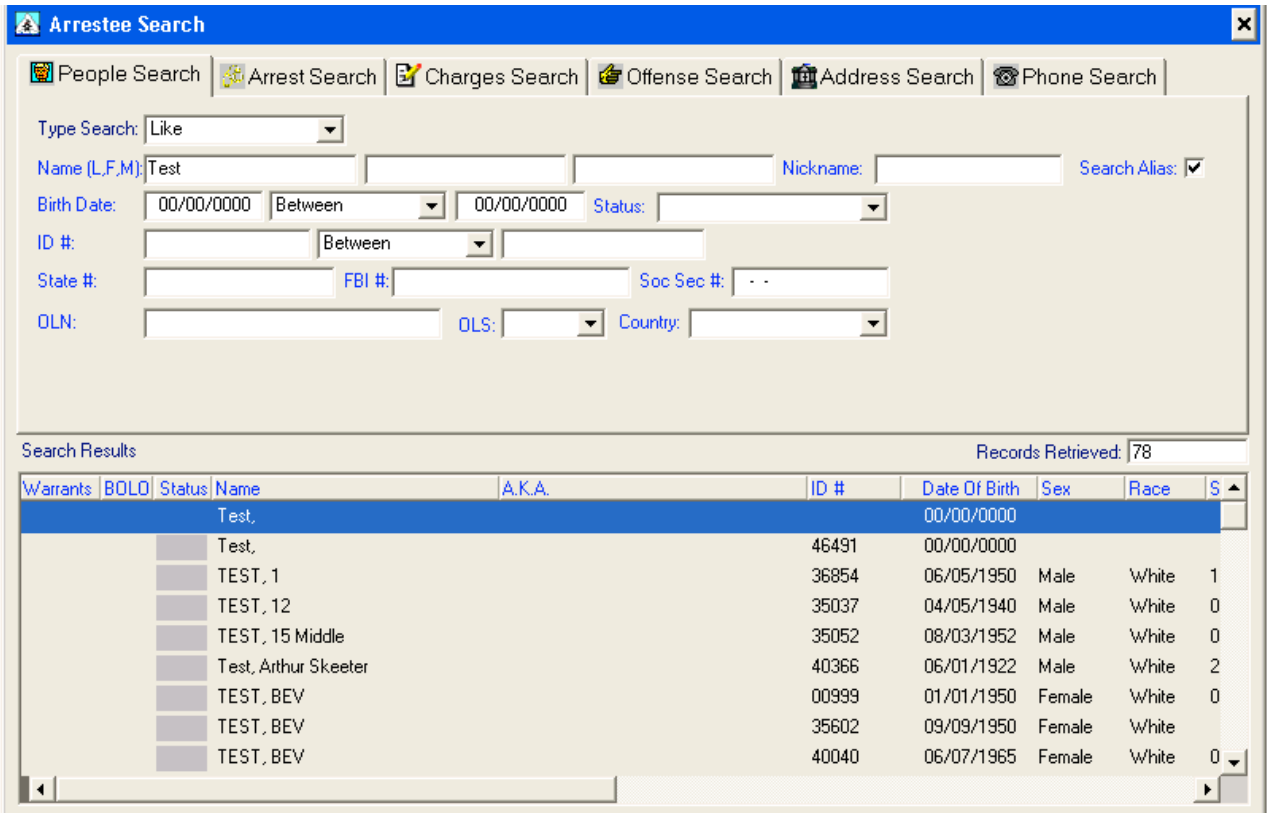
The second mechanical feature that administrators employ is the use of system logs. Every activity that a person performs using a computer or other DST is tracked and recorded; these logs are then audited on a regular schedule. The logs include two different means of observing the activities of users. First, all keystrokes and functional activities are recorded in a text file. Secondly, the system automatically takes a screenshot every five seconds and links each screenshot with the activities recorded in the text log.[61]

There are many oversight features that have been built into the local system that are fully automated and do not require any human intervention whatsoever. These features automatically cross-check and validate data that is being entered or manipulated in the system. For example, after initial entry of a suspect's data during the booking process, the system presents the booking officer with historical records that are already in the system and are likely to be the same suspect being booked. This is illustrated below using a dummy search for someone whose last name is "Test." As can be seen at the bottom of the screen, even with this fake search, the system presents multiple options to choose from.

---

[61] A 'screenshot' is a still image take of whatever is on a computer screen at a moment in time. These are sometimes referred to as 'screen scrapes'.

Illustration 20: Arrest record search results



Suppose that this was a real case, and the officer determined that one of the options provided was, in fact, the citizen being detained. In this case, the officer could click on that option and it would pre-populate the booking screen with the historical data. This is illustrated below.

Illustration 21: Arrest record detail

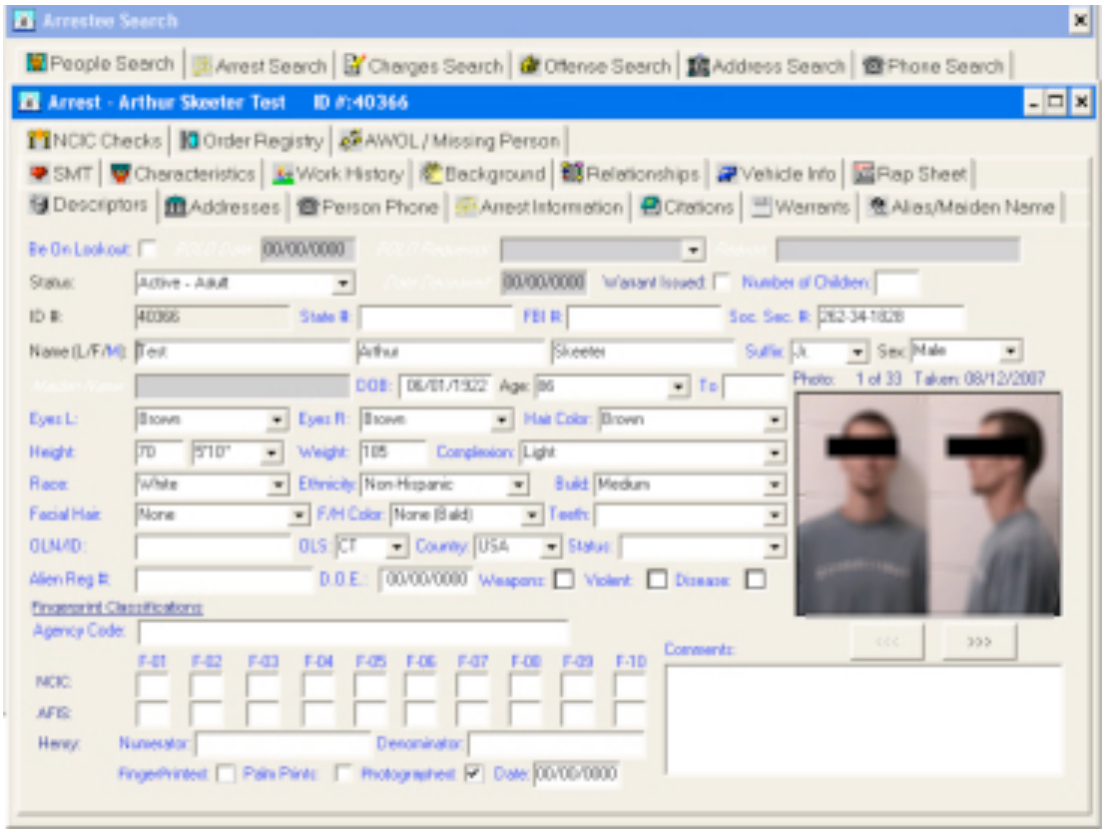


Illustration 22: Booking screen

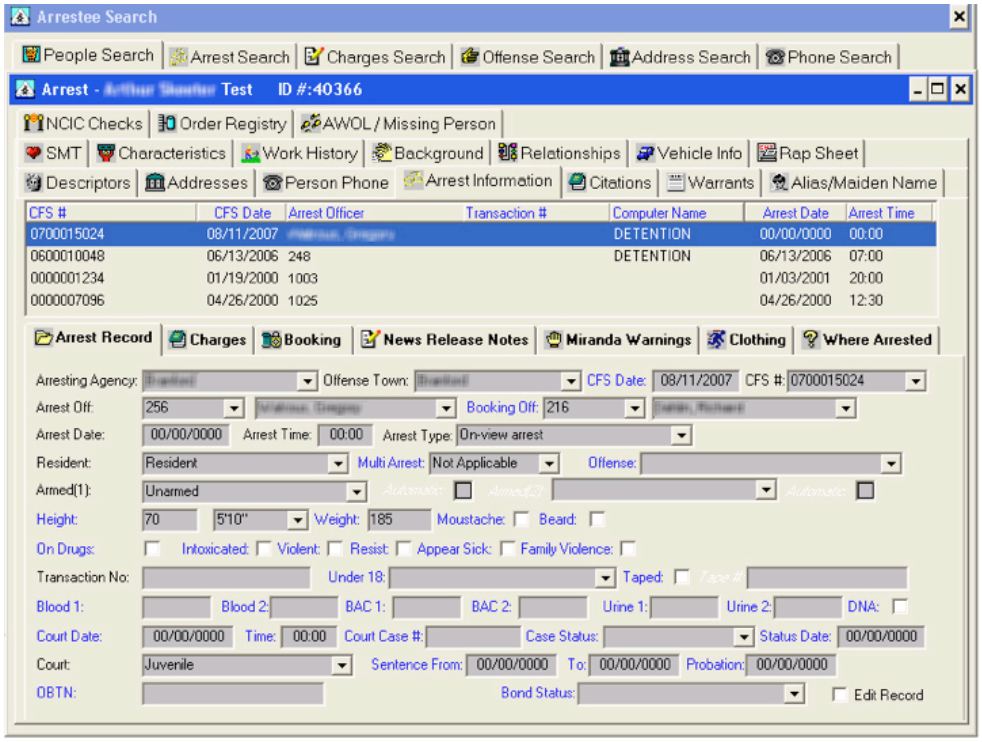
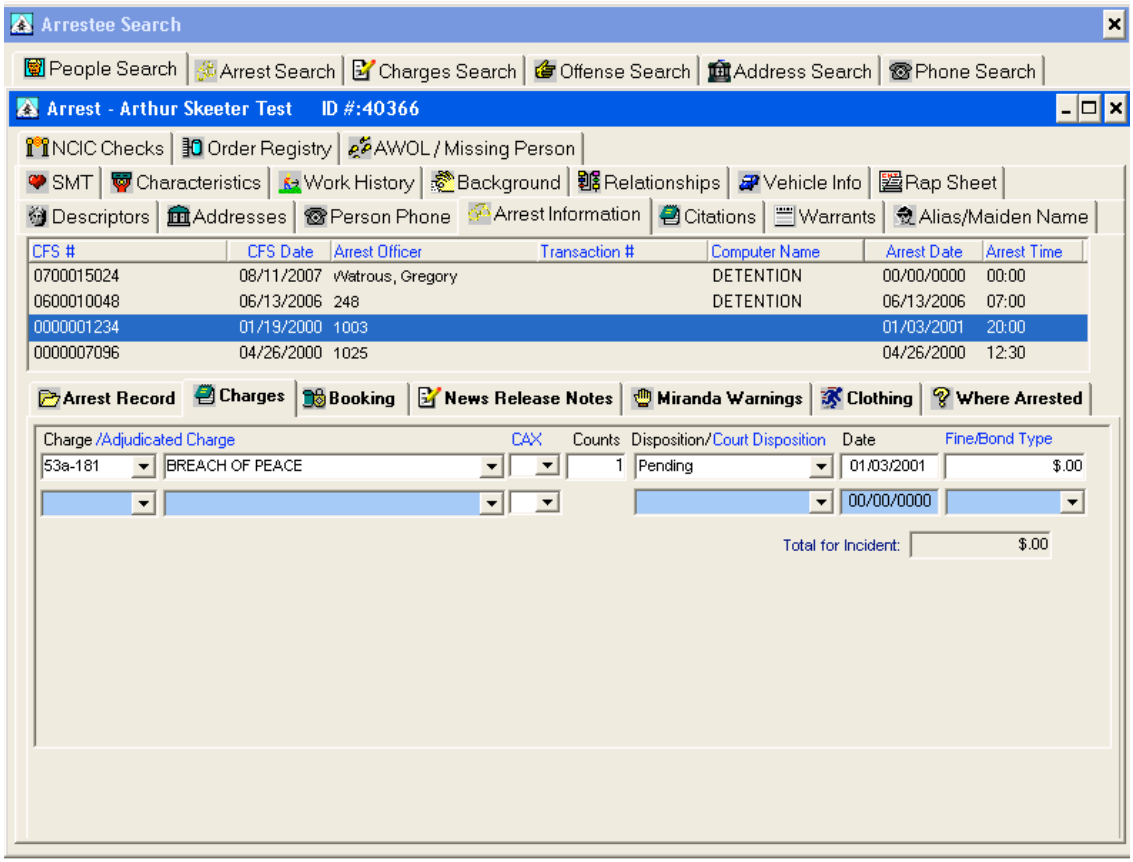


Illustration 23: Charge entry screen



From here the officer can then add new or additional data. For example, each new booking requires a new photograph to be taken and connected with this particular arrest. The officer can also search the suspect's arrest history during the booking process. This serves several functions. However, the administrators of the BPD are most concerned with officer safety. "We may have picked this guy up for shoplifting, but we need to know if he has any priors for violent offenses or what have you," the Chief explained. "Moreover," he continued, "we need to know, if possible, if the perp has a history where he might hurt himself as well."

"Across the country the problem of identity theft has been on the rise," stated Detective Travis; "Most disturbingly, this occurs where an offender uses the identity of a family member or friend as a way of avoiding being held or detained." The BPD's system has a means to mitigate

the “borrowed identity” ploy. After an individual is initially processed and photographed, they are then fingerprinted. The individual’s prints are transferred to a computer connected to the U.S. national Integrated Automated Fingerprint Identification System (IAFIS). IAFIS is the FBI’s centralized record management system for fingerprint data. In this way the suspect’s fingerprints and local records are cross-checked with the FBI’s. If the prints from the suspect and the FBI’s database don’t match, then the system indicates that within moments.

There have been very rare cases where this has occurred and it turned out that the computer was wrong. Each time, however, it was determined that the suspect being booked was actually the victim of identity theft. In a previous case in another jurisdiction, someone else, pretending to be the currently arrested suspect, was processed and printed. Individuals to whom this happens have a big problem. In addition to the legal problems of their own arrest, they have to go through the state Attorney General’s office for the jurisdiction where the ID theft occurred and follow what is likely to be a Byzantine process to get the prior false charges expunged.

Another important example of an automated cross-checking and validation process concerns judicial data held locally and by state and federal authorities. Three times a day, the BPD’s system validates its local records with the records held by various judiciary authorities regarding promise to appear, appearance bonds, DUIs, warrants, and adjudications.

Exogenous oversight mechanisms

The federal and state databases that are included in the BPD’s distributed DST network have their own mechanisms for oversight. These mechanisms are similar to those employed by the BPD, with a few striking differences. First, both state and federal entities require local agencies to agree to follow certain protocols. Moreover, the state goes a step further and requires any individual who has direct access to their database to become individually certified. The

responsibility for ensuring that local agencies adhere to the rules is largely put on the local authorities. The local administrators have a strong incentive to do so, because the BPD's certification (as an agency) to use the federal or state's systems can be stripped away by the providing agency because of the unlawful acts of one individual.

No one at the local level knows for sure what leads to an inquiry by the state or federal authorities. Dan explained, "I get a sinking feeling when they reach out to us… who did what wrong and what kind of mess do we have." The typical length of time for an inquiry is about three business days after the questionable activity has occurred. However "no one really knows for sure how their 'flags' are raised, just that it happens after the fact." Typically, they want to know why someone did a DMV search on a celebrity or political figure. Another type of inquiry is when someone checks the records on the alias for an undercover officer - "usually narcotics" - or their vehicle. "I suppose this is because there have been cases in the past where officers used these systems to give information to the bad guys." Nonetheless, "in all but one case" (which was detailed earlier in this chapter) the BPD and its officers have been found to be acting within the bounds of the guidelines and protocols.

Chapter 7: Discussion and conclusion

The overall purpose of this embedded and inductive ethnographic case study was to explore and describe a typical police agency in its everyday use of digital surveillance technologies (DSTs). By working in direct collaboration with the agency and its employees, and with the approval of senior agency leadership, it was anticipated that the researcher would, through his continual presence, gain a complete understanding of how the agency chose, implemented, and employed digital surveillance systems for both the routine and critical functioning of the agency; and, importantly, what mechanisms of oversight are subsumed into the systems. These research goals, as the previous two chapters demonstrate, have been achieved. The carte-blanche access afforded by the agency and the willing collaboration of its employees were the building blocks of this project's comprehensive ethnographic foundations.

This research and the questions that it was designed to answer was couched in two thematic arenas- one practical and the other theoretical. The practical issue was: How did a local police agency apply mechanisms of oversight to either prevent or detect unwanted behaviors and harms associated with the use of its DSTs? The theoretical issue was: Is the Situational Crime Prevention model, as Willison (2008) contends, applicable within the domain under study?

The purpose of this concluding chapter is to discuss what the findings contained herein mean as they relate to the research questions that have guided this research; furthermore, this chapter identifies specific policy implications, practical and theoretical contributions of this study, study limitations, and lastly, directions for future research.

A necessary requirement of this inductive study was to start the data collection using a protocol of inquiry which was derived from the research questions; however, obtaining information was not a linear process.

The collection of data, which began in June of 2008 and largely concluded in February of 2009, spanned a diverse range of methods. The researcher conducted interviews with and directly observed the activities of the Mayor, Police Commissioners, Police Chief, Deputy Chiefs, ranking officers, detectives, 9-1-1 operators, and clerical staff. The researcher observed multiple 8-hour shifts in the 9-1-1 call center, the booking of arrestees, routine maintenance of the web and data servers, witnessed the installation and testing of a major upgrade to LEAS, and the management of digital and traditional evidence by detectives. The researcher also attended civic meetings, staff and COMPSTAT meetings and many other daily activities.

The empirical components of this ethnographic study often presented themselves organically. The police department is an active environment. Emergency calls, impromptu staff meetings, emergent community issues, and politician consults take unscheduled hours out of every day. Many interviews and discussions with employees and staff were cut-short, only to be picked-up at a later date. This “embedded” researcher could be reviewing project memorandum one moment and in the next be brought on a “ride along” to see how to the new “dash” cam with wireless back-up worked.

Importantly, archival records, spanning a range of time beginning in the present and going back to the 1970s, were reviewed. This included a combination of newspaper reports, budget documents, still and video imagery, server logs, technical specifications, receipts, internal memos, and design notes.

The combination of interviews, observations, and archival records allowed the researcher to triangulate these sources and thus validate his findings relative to each other. It came as a surprise to the researcher how frequently the sources independently supported one another, lending validation to the empirical portrait of the BPD's use of DSTs. Beyond this, however, in an iterative and inductive project such as this one, the ability to efficiently contextualize the data is paramount. Of particular help to this endeavor were two factors:

- *Access to principals:* Because BPD turnover is slow, several of the ranking officers who collaborated in this study, including Chief Sowley, have been at the BPD since before the first DST was constructed in the late 1970s. Collaborative and cooperative access extended to Belleville's Mayor and other officials outside the BPD. Uniformed and civilian staff collaborators contributed substantially as well since more than half of the current officers and over 90% of the clerical staff has been at the BPD since LEAS was first introduced.
- *Centralized archives.* The BPD's archival data is located on premises and is well-organized. Unencumbered access was granted. Thus, this researcher was able to use original source documentation to cross-reference and cross-validate information obtained from interviews and direct observations.

Each of the three preceding substantive chapters amalgamates data exhaustively collected and triangulated from interviews, documentation, and observation. Even so, within each chapter, different sources took on varying importance. For example, chapter five, which covers the development of DSTs in Belleville from the 1970s until the present, relied heavily on interviews and archival data.

One of the more interesting interviews was impromptu and came after a COMPSTAT meeting that the researcher observed. In that case the researcher was casually speaking with Officer Dorrance, who has been with the BPD since the early seventies and had also been a volunteer fireman and EMT. This officer was a HAM radio hobbyist and had redesigned the radio and pager systems when they had integrated all of the Emergency Services in the mid-nineties. Now, he manages the operators in the 9-1-1 call center and was a key collaborator in this research. This officer had a near-photographic ability to recall dates and circumstances and directed the researcher towards a number of concepts, documents and lines of inquiry that contributed significantly to this research, particularly Chapter 5's historical review of BPD systems.

Chapter 6, which covers the current status of the DSTs, made extensive use of the technical specifications and documentation as well as direct observations of the systems in use. Direct observations would often take place while employees were using some aspect of the system for their job; moreover, during those times the researcher would be asking questions about what the employees were doing and how the system worked to support their tasks. Photographs were taken and screenshots were captured, often at the same time, to further contextualize the collaborators portrait of their DST work world. In the DST environment under analysis, whether the screenshots and user logs constitute direct observation, documentation, or some hybrid of both is a matter of methodological debate. Regardless of that debates resolution, the photographs and screenshots provide needed context for an overall understanding of the domain under study.[62]

---

[62] All images contained in this document appear with the expressed consent of the BPD. All photos and images were screened to ensure that no data or content was shown that is explicitly prohibited by state or federal law. Places where

Probably the most interesting part, for the researcher, of the direct observations was to see, in real-time, the controlled chaos of the 9-1-1 operations center. A typical shift, where the researcher was present, had three call operators working.

On a typical call the operators are dealing with the caller, first-responder and back-up units, and information look-ups in the database. Calls may be passed on to another 9-1-1 dispatcher. Similarly, the researcher, when observing and speaking with the 9-1-1 operators, was sometimes passed from the one to the other in order to get more complete answers to questions he had posed. This distributed work, shared expertise and mutual support was the reality of working in that environment. It was no less necessary for this researcher, who was embedded in that environment, to "go with the flow" in order to understand as fully as possible how those employees, and their systems, functioned. Their particular place in the operations and direct access to nearly all of the DSTs was of tremendous aid to the researcher. No one uses the system more or has as much insight into the minute-by-minute "pulse" of the operations as those operators.

Analysis of findings

Qualitative research is inherently complex. The methods of gathering and analyzing data and determining its value can be done in innumerable ways and there is no one "right way". And, while the analytical stratagem is outlined in the Methods section, chapter 3, some points are worth reiterating here.

---

the screenshot includes identifying data were blurred to protect identities.

The researcher embarked upon this study cognizant of multiple concepts and propositions bearing upon the subject matter from sociology, criminology, criminal justice, and computer science. Moreover, that intellectual backdrop was also punctuated by concepts from the canons of surveillance studies, systems auditing/oversight, and Situational Crime Prevention (SCP).

Analyzing the findings was a highly iterative exercise that involved numerous follow-up interviews, document searches and having key principals and other collaborators at the BPD read this document at various stages of its development. It is crucial to point-out that connecting the dots in an embedded case study such as this requires not only multidisciplinary knowledge but also an experience base incorporating the creation and maintenance of such systems. To that end, the researcher also relied on his professional expertise as a designer and auditor of complex data and digital surveillance systems as an important analytical anchor.

Below the key findings from this research are outlined and discussed in a thematic way but the presentation of themes below is <u>not</u> meant to imply a hierarchy.

Incremental, employee-driven innovation

This research began with the assumption that its focus would be on the current status of the BPD's digital surveillance technology systems—a very significant installation that has been the model for 40 other jurisdictions in the state. As the research began it became exceedingly clear that understanding why the system is what it is, today, required an understanding of preceding systems, including the seminal efforts of the late 1970s. As has been illustrated by this research, the development of the locally-created system was an evolution of trial and error and success that spanned many technology leaps and evolutions over a period of almost thirty years.

This researcher, whose background includes systems development, was surprised to find how technologically advanced the system had become. Normally, development of a distributed

network, like the one under study, is orchestrated by engineers working with business and domain experts to create a comprehensive development protocol. Here, however, the entire system was primarily constructed by two cops, one a software hobbyist and the other a part-time software engineer and part-time cop; moreover, they did not start with a grand strategic plan but with the idea of automating redundant and time-consuming tasks in their agency.

Thus, the 30 year development of Belleville's DSTs is a story of innovation and practicality. The core data system, LEAS, is an impressive amalgamation of serendipitous choices made over time in an environment of shifting legal, functional, and procedural demands. It was developed with limited resources and, mostly, on time that was not directly compensated for. And yet, what was built not only endured over time, but actually became a model directly adopted by other jurisdictions

Pervasive integration of DSTs

The adoption of DSTs at the BPD has resulted in a distributed network of data acquiring, sharing, and management tools with a nationwide reach, though the core system remains the BPD's homegrown LEAS. Today, all facets of running the BPD are tied into LEAS, which in turn ties into the federal and state law enforcement networks. As this research project comes to an end, every single routine, administrative, or critical function of the BPD is facilitated by, or fully supported through, the agency's network of technologies.

The centrality and reach of BPD's systems fully comport with the predictions of some (Rule, 1974; Wood, 2006; Wright, 2005; Zureik & Salter, 2005) as well as the concerns of others (Garland, 2001; Los, 2004; Lyon, 2003a, 2003b; Marx, 2002; Rhodes, 2004; Stanley, 2004). Notwithstanding those concerns, there is little doubt that the level of DST sophistication and

penetration that the BPD has accomplished will be replicated in police agencies large and small in coming years.

The Human Operators Matter

The pervasive adoption of technologies should not mean a diminishing role for police officers. This case demonstrated quite the opposite from the development of the system to its' use. This study found that trained police professionals can best make sense of the quantity and variety of data DSTs provide. As the bank robbery case illustrates, crime patterns may only be discernable when viewed over time and across space as data accumulates relative to suspects, and a professional eye with a multi-jurisdictional view is critical.

With digital technology increasingly mediating public intercourse in modern society, police, to be effective, have to adopt and integrate appropriate digital surveillance technologies. The presence of these technologies, as advanced and efficient as they may be, is not sufficient. Properly authorized officers and investigators must have access to all that the digital toolkit provides, and must be trained in the lawful use of these digital surveillance tools. Then, ethically aware criminal investigators can use DSTs to apply the 'fuzzy logic' of their professional training and operationally-based intuition to piece together non-linear and disparate crime puzzle pieces.

The bank robbery case underscores another critical issue for the effective utilization of DSTs; namely, the de-centralized and fragmented reality of policing in the United States. The centralized data systems of state and federal criminal justice authorities go a long way toward making the accessing and sharing of data more efficient. This, however, does not obviate

significant problems that still attach to control and access to data held by local jurisdictions, or cumbersome requirements for accessing state and federal data.

Though the bank robbery case originally was being managed locally, the investigator sought federal help when he recognized a cross-jurisdictional pattern and suspects living beyond their discernable means. Initiating FBI involvement brought rapid access to IRS records and additional data resources. Had the investigator not called in the FBI—the amount stolen had not reached the threshold for automatic FBI involvement—accessing IRS data would have been a slow-track process requiring multiple approvals.

The installation of the GPS tracking device on the suspect's vehicle involved less formal cooperation between state and local agencies. The investigator arranged to have the suspect's parole officer call him in. The GPS tracking device had been borrowed by calling in "a favor" from a detective at a neighboring police agency. The BPD investigator and a detective from yet another jurisdiction, in which the parole office was situated, installed the tracking device. DSTs, however sophisticated, still operate across a jagged terrain that divides agencies in different jurisdictions and levels of government, and it often takes individual law enforcement personnel to creatively bridge those divides.

The findings that emerge from this case belie assertions those who posit that DSTs themselves, networked to a host of data collecting and data analytic systems, impose a logic on law enforcement executives and operators that impinge on citizens privacy and other rights even when such systems are lawfully used (Ericson & Haggerty, 1997; Lyon, 2007a; Marx, 1992b). What was found here was an executive staff that role-modeled prudence, carefully trained the system's users and embedded controls and safeguards into the system.

Effective oversight as unintended consequence

This inquiry's central concern was the oversight mechanisms built into DSTs used by the police agency under study. The BPD created, without a long-term development plan, a robust and technologically advanced data collection and management environment. The controls and oversight mechanisms built into this environment are no less robust, advanced and effective. In general, designers of technology systems such as Belleville's attribute unplanned positive outcome to a string of "happy accidents." This, to a large extent, is the case in Belleville, though these controls and oversight mechanisms are now formally recognized as protections against abuse, as well as devices to promote efficiency and minimize errors.

The data that is collected and used within the distributed network of DSTs are highly controlled. Multiple over-lapping and redundant oversight mechanisms exist to prevent unauthorized and illegal uses by law enforcement personnel. In the agency under study, oversight is based on a preventive model that relies on technology as a delimiter of behaviors. When agency personnel input data into the system, various techniques and procedures automatically cross-check and validate entered data with historical data from local, state, and federal records. These reconciliations reject most inaccurate entries and circumscribe a range of unwanted behaviors or outcomes. For instance, the potential for inappropriate vehicle stops or false arrests is minimized since LEAS checks state judicial records three times daily to update its local files on warrants, wants, and adjudications.

When personnel are accessing data held by other local, state and federal agencies, fewer automated checks are in place. Here the BPD relies on a "trust, but verify" model, and a cooperative partnership with providing agencies to root out misuse. When anomalous inquires or usage patterns on exogenous systems are detected, as was described in the previous chapter, calls

are made by state and federal agency authorities to the appropriate BPD official, and corrective action is swift since access to the exogenous data source has been put at risk.[63]

The confluence of these various checks and balances yields an environment where the local law enforcement agency is strongly mandated to minimize, and its employees are firmly directed to refrain from, improper uses of the system(s). In fact, the DSTs and computer systems of the BPD are subject to a level of scrutiny and regulation that seem custom-built for the protection of citizens' rights and compliance with law and regulation. On the whole, the police and the community reap the benefits of the public safety activity embedded within this particular DST installation; while also being spared oppressive social control and negative externalities from system misuse.

This positive outcome for civil liberties and lawful use of the system was more serendipitous than planned. The designers of the system neither intended nor constructed their technologies to enhance civil liberties. Instead protections for civil liberties were an unintended consequence of the rigorous oversight built into the system to avoid error and increase productivity. Paper forms are time consuming and error generating. Auto cross-checking online forms delimits errors and get cops back on the beat. Similarly, written reports are not the forte of the average officer. So dictated reports with clerks typing the transcript into the system achieves the same kinds of efficiencies.

As Chief Sowley explained, "To tell you the truth oversight was never really our main concern, I mean, we started with the baseline of what the state and federal rules were but our main emphasis has, and continues to be, efficiency".

---

[63] Depending on the particulars of the circumstance that official may be the mayor if the concern is about the activities of the Police Chief or Deputy Chief.

Sowley's statement comports with the views of other surveillance scholars regarding the police and their adoption of technologies (Gandy, 1993; Garland, 2001; Marx, 1988, 1992b, 2002); namely, that the police are focused on adopting increasingly more technologically advanced communications and data management systems with a focus on efficiency. However, the present study also produced findings at odds with another conclusion reached by these scholars--that the technologies adopted by the police will necessarily lead to a more intense forms of social control. Citizen safeguards were built into these systems, however serendipitously, and now have become formalized at a level that provide Belleville citizens with more, not less, protections against erroneous and arbitrary surveillance and control by law enforcement. These systems checks and audits complemented the culture of prudent and proper use of the system hat the BPD has instilled in its' personnel.

Dismantling the 'harm opportunities' using Situational Crime Prevention [SCP]

An important part of this inquiry, crossing both theoretical and practical domains, can be identified in the final research question which asked: "Can a harm-reduction and preventative mindset such as the SCP approach lead to the design of policies and protocols that better guard against externalities and, if so, what specific protocols or policies could be employed?"

There are several aspects of this question that should be addressed. First, it was argued by Willison (2008) that SCP could be used to control behaviors in an information system. His argument, however, was not empirical, per se; rather, it was conceptual. He did not go into the field a look at a specific information environment to assess whether his premise(s) were true. That said, what this research finds is that Willison *is* correct- SCP can be useful in this regard. However, that doesn't completely answer the question posed.

As identified in chapter 2, Review of the Literature, the techniques of SCP are intended to be a 'toolkit' from which particular instruments can be brought to bear on a specific problem in a specific environment. What Willison (2008) does not provide, and this research does, is useful direction on how that might work in a specific kind of environment, local law enforcement agencies, where the use of DSTs that allow flexibility and have effective oversight mechanisms is crucial to their core mission and also making sure that boundaries are not overstepped.

The need to disseminate effective strategies for insuring the law enforcement data system's integrity was underscored by several events as this study drew to a conclusion.

First, the National Institute of Justice released a report on technology priorities for criminal justice agencies (National Institute of Justice, 2009). And while the report, which is aimed primarily at state and local agencies, identifies interesting ways that agencies should employ DSTs, it is silent on the issue of oversight and accountability and restraints upon system misuse.

Second, in January of 2009, the Supreme Court ruled on a case involving the arrest of a citizen based-on outdated information ("Herring v. United States," 2009). The plaintiff argued unsuccessfully that the "good faith" exemption for officers in this case should not apply because the police were negligent for not maintaining current digital records. The warrant for his arrest was rescinded months prior to his arrest. In her dissent, Justice Ginsburg argued that there is a "systemic risk" of error in distributed networks of data held by law enforcement where the data is not cross-validated and the ramifying effects are unknown. Thus, she wrote, the police that use these systems but do not employ the basic technologies to circumvent errors are negligent and should not receive the 'cover' of "good faith" when errors are made based-on faulty data that is verified when it could be.

Third, a May 2009 audit of police abuses of data systems in Massachusetts (Auditor Of The Commonwealth, 2009) showed a pervasive pattern of abuses by law enforcement officers who used the system's expansive data collection for unauthorized inquiries. The report also makes clear that effective procedures and technologies to track and/or delimit uses of the statewide databases are not present. Consequently, once inside the system anyone can view, alter, or destroy data with impunity. Commenting on the Commonwealth Auditor's report, some experts argued that this is a pervasive problem in law enforcement and in other fields, especially health care (Moscaritolo, 2009).

Belleville, and presumably other jurisdictions adopting its LEAS, does not have this level of vulnerability to purposeful abuse or system error. As this research has shown, anomalous uses of the system are identified in real-time, and improper uses are swiftly and firmly addressed, regardless of rank. The sentinels are effective, even if not originally developed for guardianship purposes

So how does the practitioner or researcher examine a digital records or surveillance system in order to yield the information necessary for that system's security to be assessed and enhanced in accordance with SCP principles?

Earlier, this report identified how the SCP approach directs practitioners to "dismantle" the "harm opportunities" in an environment (Sparrow, 2008) and also identified the many ways that this approach had been applied.[64] Previous approaches, however, involved 'traditional' crime issues and were applied by legal authorities to prevent unwanted and illegal behaviors by citizens. It was an open question whether or not, and in what ways, SCP could be useful in the DST environments operating in law enforcement agencies.

---

[64] See chapter 2

A primary goal of the research was to determine how "offenses" by law enforcement users were, or could be, prevented or controlled and how harms from employee offenders were, or could be, minimized. The researcher posited that Situational Crime Prevention principles had promise in this regard. DSTs present a complex terrain of interconnected nodes built to facilitate socially desired public safety purposes. But these complex and decentralized systems also present insiders with opportunities to commit unauthorized, unlawful, or socially destructive acts. The overall social utility of the DSTs is a function of how these social 'goods' and social 'bads' balance out and, sometimes, clash. SCP concepts can be used to dismantle the opportunities in the digital environments that give rise to the harms (or 'bads') while still permitting the 'goods' that the system enables, namely highly effective policing that prevents crime and lowers the fear of crime.

The assumption built into a digital SCP approach is that more transparency and increased oversight of the ways these systems and their data are used would necessarily lead to a decrease in harms. "Sunlight," As Justice Louis Brandeis's observed "is the best disinfectant," to which this research adds "… and deterrent."

To assess the increased oversight proposition, the researcher developed an information collection protocol for fully understanding the DST environments under study (see below).[65] However, it became apparent early on that the initial protocol needed refinement in order to assess the lengthy and circuitous development path of the various elements within Belleville's distributed DST network.

---

[65] The protocol introduced in this research is an elaboration on a protocol the researcher developed with Dr. Peter Mameli of John Jay College of Criminal Justice.

Throughout this endeavor the researcher discovered numerous instances where the DST environment itself, as well as agency protocols for its use seemed to be purposefully derived from SCP protocols. It *appeared* as if the designers of the local system were basing their overall system scheme on the environmental scanning and embedded preventative principles of SCP. This appeared to be the case because so many of the features and mechanism designed into the local DST system could be linked to the "25 techniques" of SCP. Below are but a few examples of DST elements at the BPD that are imbued with SCP ideas (implicitly) but were explicitly put in place in order to achieve a different objective.

- **Increasing the effort**
  - *Passwords.* Are de facto forms of target hardening and controlling the access to the system; however, they are also necessary as a basic tool to identify the user and therefore make sure that the individual user has access to the elements of the system they need in order to do their job.
  - *Passkey.* Each employee has an electronic passkey that attaches to their keychain. Getting into sensitive areas such as the jail, booking, evidence room, the Detective Department, and the data server room requires the use of the passkey which then records who entered the room and when. However, the purpose of this feature is to prevent non-police personnel from getting access rather than as a form of internal controls on employees, though that, in fact, is a direct consequence.
  - *Automatic logout.* When a workstation has been idle for 5 minutes it automatically logs-off. This is a standard feature in most computer environments and is meant to compensate for a very human weakness, forgetfulness.

- **Increasing the risk**
  - *Logs.* The computer logs all of the activities that a user engages in while using the system. This is actually a core function of the server technology and it was not developed by the BPD. Also, the original purpose for the log feature was to assess glitches rather than to oversee users' activities. Similarly, the visual logs (preserved screen shots) were originally meant as an additional back-up in case records needed to be restored in the event of data loss. Nonetheless, these features also track any given user's path through the system, recording all behaviors whether "over the line" or benign.
  - *ISYS.* ISYS, which has powerful search features, is situated so that any user is in plain sight of supervisors and peers; however, this is consequence of the license agreement with the provider, which only allows one workstation to have the software installed. Thus, its prominent and centralized location in view of other users of the system serves to prevent abuse.
  - *Surveillance cameras.* Are located in, and observe, sensitive spaces, such as the jail and evidence area, as well as the forward view from the dashboard of police cars. The intended purpose of these cameras is to indemnify the BPD against accusations of police misconduct, but they also have the effect of deterring police misconduct.
  - *User names.* One cannot log into any computer without a username (which is also tied to a password). Like the password, this allows administrators to manage the features made available to individual users; but also serves to restrict access on a

"need to know" basis. This reduces the opportunities for casual or compromising intrusions by agency personnel at large.

  - *Clerical staff.* The use of clerical staff to finalize reports for officers is intended to efficiently get police back 'on the beat'; but also serves as a quality control review.

- *Administrative change alerts.* The primary systems administrator, Lieutenant Dan, is responsible for daily operations of the DSTs in Belleville. However, the Deputy Chief has the same administrator rights. Whenever there is a change to a user's account granting or denying them access to particular features, an alert is sent to both DST administrators. The double alerts are meant to facilitate communications. If Dan provides additional access to Officer Smith he does not also have to email the Deputy Chief. However, this also provides a mechanism for redundant executive review of changes in access privileges
- **Reduce rewards**
- **Reduce provocations**
  - As Willison (2008) anticipates, the two SCP elements above had little applicability in the DST environment under study.

- **Remove excuses**
  - *Explicit policies posted.* The BPD has explicit, detailed policies covering the appropriate use of DSTs. Before Sowley became chief in 2006, these rules were less extensive and primarily mirrored the state's posted rules. However, after an executive officer was caught misusing the state database, the BPD sought to

increase the rigor of its local governance of DST use. An upcoming CALEA audit of the agency was also a driver for the agency updating its DST rules. Explicitly articulating the rules, posting reminders of the rules and requiring employees to annually certify that they have read and understand the rules significantly reduced excuses for aberrant behaviors.

- *Mandatory Training.* Each employee must be trained and certified to qualify for access to the state databases.

Though the designers of the DSTs in Belleville were not trying to "dismantle" harms as much as increase efficiency, the design of the system incorporates elements that deter purposeful misuse and reduce accidental errors that can harm citizens. The mechanisms now in place 'track' well with the existing principles of SCP, thus validating Willison (2008).

Though the motivation for, and the results of, the SCP-like innovations in Belleville may have been divergent (yet more consciously convergent in recent years), this research points the way toward protocols for assessing an existing DST system in order to determine whether the system is sufficiently equipped to prevent abuses and accidental misuses by insiders. These protocols could be used by researchers and executives without a technical background. These protocols are also informed by this intensive case study of Belleville's DST installation and significantly extend existing SCP literature as it pertains to deterring harms in digital environments.

The protocol consists of a series of questions to help law enforcement organizations determine their current state of governance and oversight with respect to DSTs.

The questions are meant to provide knowledge for action in order to harden internal transparency, accountability and oversight. The instrument can be applied at any time during the life cycle of an organization's DST systems in order to provide a snapshot of its internal surveillance management environment. Remedies to problems identified are expected to differ by entity. Therefore, prescriptions for correction must be written by the organizations in question. However, the nature of the questions strongly directs those implementing the protocol toward certain types of mechanisms that can be used to strengthen their governance measures.

The proposed protocol is detailed below.

1) What external agencies are charged with carrying out oversight of the surveillance technologies you create and/or work with?

   Please name the oversight agencies and explain their roles.

2) What internal units within your agency are charged with carrying out oversight of the surveillance technologies you create and/or work with?

   Please name the oversight units and explain their roles.

3) How is oversight carried out for the surveillance technologies you create and/or work with? Please explain for each condition noted below and differentiate by type of technology if necessary. Also, please provide documentation if possible.

   A) Consultation with experts beyond the project team?
   B) Closed/open hearings within the organization?
   C) Closed/open hearings with the public or an oversight body?
   D) Program evaluations of implemented technology?
   E) Performance audits for accountability?
   F) Financial audits for accountability?
   G) Investigations of fraud, waste, abuse and mismanagement?
   H) Ongoing performance measurement system development and monitoring?
   I) Other

4) Are experts external to the project (either inside or outside or your organization) utilized to ensure that the surveillance technology being constructed satisfies appropriate ethical concerns for development and implementation? Please explain.

   What about regulatory concerns? Please explain.

What about statutory legal concerns? Please explain.

5) If your agency issues a Request for Proposal (RFP) for development of a surveillance technology, or employs a subcontractor for such a purpose, what accountability mechanisms (if any) do you require to be built into the resulting submissions? Please explain.

6) Does your agency establish performance measures in its contracts when dealing with the creation of surveillance technologies?

   If yes, please explain the steps, benchmarks and measures that are to be built into the contract for provision of such services to determine if a vendor is effectively achieving desired outcomes.

   Also, if yes, please explain what happens if a vendor or subcontractor fails to perform adequately.

7) If you do not currently establish performance measures in contracts where surveillance technologies are concerned, do you think that this is a good idea for the future?

   If you do currently establish performance measures in contracts where surveillance technologies are concerned, how do you think that this process could be improved?

8) Does your agency have an articulated rule defining inappropriate and/or personal use as it relates to surveillance technologies and information databases?

   If yes, please explain and/or provide a copy of the rule.

9) Suppose someone is suspected of misusing surveillance technology or information databases? Is there a formal process for investigating and adjudicating the breech?

   If yes, please describe the process and/or provide a written copy of it.

10) What systems do you have in place for actively detecting potentially inappropriate or personal uses of your surveillance technologies and databases?

    Please explain how this is done and if you utilize an automatic alerting of suspected misuse anywhere in the system.

11) What systems do you have in place for receiving information from individuals about inappropriate or personal uses of your surveillance technologies and databases?

    Please explain how this is done and if you have established a system of “whistle-blowing” protections for people so that they feel they can alert managers and other relevant parties when misuse is detected?

12) If 3rd party vendors build, implement, or help operate your systems, how does your agency ensure that the vendors and their employees don't re-use or re-sell the code, access the system for unauthorized purposes or otherwise violate policies governing the system's use?

13) How does your organization secure proprietary algorithms for its surveillance technology activities?

    Please explain and/or provide written copy of the process.

14) If your organization procures third party algorithms for surveillance technology, do you have a process for checking the validity and reliability of the algorithms?

    If yes, please explain and/or provide written documentation of how this process works.

15) If your organization procures data from third-parties, how is it securely stored when the original purpose for its use is completed?

    Please explain and/or provide written documentation of this process.

16) Considering how information and databases can be re-purposed and mined for a near-infinite number of applications, how do you ensure that the systems you implement are not turned to other purposes that cross legal or ethical boundaries?

    Please explain and/or provide written documentation of this process.

Digital evidence validation

The DST system built and employed by the BPD has an Achilles' heal. The data collection and management system(s) were designed to support traditional police issues and, importantly, tended to mirror traditional, paper-based approaches to documenting and tracking data. However, only in the last ten years has the use of digital technologies by the average citizen reached critical mass. Increasingly, evidence used in criminal cases is gathered from some kind of DST. In the bank robbery case described earlier, nearly 100 percent of the evidence came from digital sources, including GPS, CCTV, and cell phone logs. With evidence that originates

or is managed digitally there exists the possibility that someone may change or manipulate the data to make it appear more incriminating.

While the bank robbery case was ongoing Lieutenant Picasso demonstrated to this researcher the wealth of digital data that had been obtained by the BPD. The collected whole, from so many different sources, illustrated a clear pattern of behavior on the part of the suspects. The researcher asked Picasso "Suppose I was the defense attorney and I asked you to prove that you did not 'disturb' or distort the evidence to make my client more guilty… how would you prove that you didn't?" To which Picasso responded, "Oh, I would never do that". The researcher pressed Picasso who eventually had to concede that he wouldn't have a good answer to this in court.

This was an unexpected finding and one that may not have come up but for this case, which ended with plea-bargained sentences. The initial conversation with the Lieutenant was followed by a similar conversation between the researcher and the Chief and the Deputy Chief. They conceded that digital evidence tampering was potentially a problem. Following this discussion about the collection and management of digital evidence, the agency decided to make digital evidence experience a requirement for a new detective line being filled. In addition, the BPD has asked the researcher to develop a digital evidence policy and assist them in designing technological solutions to implementing the policy.

Accountability for the Overseers

Some elements of the digital evidence validation issue arise in the area of executive oversight of Belleville's DST's. As observed earlier, a strong culture of proper DST usage has been established in Belleville, and oversight is exercised and accountability is effectively

pursued in both formal and informal ways by ranking officers who have a long history with and/or a high psychological investment in the DST systems. But the interventions by these senior officers, while highly effective, are often poorly documented. This leaves open the question of how you hold the executive overseers of the system accountable, especially since, in the not-so-distant future, executives less-invested than the system's founding fathers and charter users will be in charge. Stronger systems for documenting oversight actions would appear to be called for.

Policy and liturgical implications

This case study was focused on public policy and the administration and management of police agencies and their use of technologies within a particular theoretical construct, Situational Crime Prevention. Frequently, a study such as this addresses the implications for policy and the scholarly literature separately. In the instant study, however, the policy and theory implications interpenetrate and overlap as noted below.

- *Complete access.* Within the canon of 'surveillance studies' literature this study is unique in obtaining complete and authorized access to *all* of the memos and documentation pertaining to the DST systems' development and ongoing management, as well as to the people who use, manage, and created the DST system. Most previous studies of DSTs in law enforcement or security organizations have typically been done exogenously (Müller & Boos, 2004; Ruegg, November, & Klauser, 2004; Sætnan, et al., 2004; Sutton & Wilson, 2004; Wakefield, 2004; Walby, 2006; Zurawski, 2004). Research conducted within agencies is typically limited to ethnographies about single DST elements such as CCTV operations. This research

was the first to study the full range of an agency's surveillance mechanisms directly and intensively.

- *Evolving and validating SCP.* This study has several implications with respect to SCP, both in theory and in practice:
  - *T*his study applied SCP in a novel way- looking at how it could be applied as a tool for governing and delimiting the behaviors of the police in their use of DSTs. What the researcher found was a *de facto* validation of the SCP approach in the digital environment. This finding is underscored by the fact that embedding SCP was not the intention of the designers of the system.
  - Typically, SCP is applied to an environment to change outsider, and outlier, behavior(s). In that vein, when SCP was applied to digital environments, the studies focused, primarily, on 'outside' offenders hacking into data management systems. This research, however, considered regulating the use of digital surveillance systems by authorized personnel *inside* the system.
  - The applicability of SCP in the information and data security domain is something has been argued on conceptual grounds. This research empirically and explicitly validated this argument for major elements of SCP.
- *Roadmap for practice.* This research serves as a useful roadmap for practitioners. All police agencies eventually will employ some version of a digital record management system. This is inevitable as the technologies become cheaper and their power increases. Thus, the development path followed by the BPD and how it addressed emerging issues can serve as a useful model for police agencies implementing or upgrading DST systems. Also, many agencies with existing systems could, but do

not, have many of the safeguards designed into the BPD's systems. Thus, this research can provide direction for those administrators who seek to audit and improve the DST accountability and oversight mechanisms in their own jurisdictions.

- *Improvements in Belleville.* This research identified gaps in the policy and practice of the BPD with respect to digital evidence collection and management. As mentioned previously, the researcher is working directly with the BPD to rectify this situation.
- *Wrong for the right reasons*. That increased technology used to create efficiencies by law enforcement will result in increased social control is a standard assumption in much of the surveillance literature. Given that this research found that technologically-mediated increases in efficiency resulted in increased oversight and accountability measures, one could argue the premises of previous surveillance research about the ever-expanding reach of DSTs are correct but the conclusions about an attendant official lawlessness are wrong.
- *Useful protocol for DST inquiry*. The protocol used in this inquiry proved to be an efficient tool for obtaining necessary and critical data pertaining to DSTs, especially with respect to understanding their measures for accountability

Limitations

There are inherent limitations whenever one conducts qualitative case study research. For example, there are the oft-cited concerns of "going native", myopia, validity, reliability, and generalizability (Tewksbury & Mustaine, 2004). That said, some of the 'classics' of criminal justice and criminological research have been case studies that resulted in theoretical and practical understandings that continue to drive research today (Anderson, 1999; S. Cohen, 1972;

Jack & Snodgrass, 1982; Liebow, 1967; C. R. Shaw & Burgess, 1930; C. R. Shaw, McKay, McDonald, Hanson, & Burgess, 1938; Steffensmeier, 1986; Thrasher, 1927; Whyte, 1943; Wright & Decker, 1994).

Within this particular study there are a certain potentially limiting characteristics that must be understood in order to appreciate the value of the findings reported in this study.

- *Generalizability.* This research focused on a single case which invites the argument that the findings are only true for the agency and circumstances under study. However, not all research need be instantly generalizable. As has been the case with this study, knowledge value is also generated by intensive understanding of signal phenomena, which then may ground further practice and research that builds towards generalizable knowledge. In addition, the theoretical generalizability critique must contend with the practical reality that the core system developed by the BPD, LEAS, has been adopted by 40 other agencies in their state. .
- *Reliability.* Even though there are 40 other agencies in the state using the same core RMS, what cannot and should not be assumed is that all 40 agencies have the exact same DST networks with the exact same arrangements of technologies or local policies. There is little doubt that when this research is extended there will be variation in both the scope of technologies used as well as the policies applied by each jurisdiction. That said, these variations should be of limited concern as long as the protocol and method for obtaining the information about a given jurisdiction's use of DSTs is, in of itself, valid. Or, as Yin (2009) argues, the purpose these kind of case studies is "analytical" rather than "statistical" generalization (See also Guba &

Lincoln, 1981). As Tellis (1997) states, "Reliability is achieved in many ways in a case study".

- *Construct validity.* Tellis (1997) reminds us that construct validity can be problematic with case study research as it undermines the validity and, possibly, the credibility of the researcher. To address this, the drafts of this document were reviewed with key participants throughout the process and multiple-sources of data were used.
- *Retrospective construction.* Events recollected and recounted after a considerable time has passed is a concern when conducting this type of research. However, this possible limitation was mitigated by the researcher's triangulating data from many sources, particularly extensive archival records pertaining to previously recollected events.

Directions for future research

The findings of this research will lend itself to multiple avenues of inquiry, these include but are not limited to:

- The role that entrepreneurship can and should play in police innovations at the local level.
- A survey of all agencies using LEAS to assess the totality of their DST networks, how they were developed and organized over-time, how they are funded, and the policies associated with oversight and accountability
- A replication study to assess the development and use of DSTS in larger law enforcement agencies.

- The further development of the protocol proposed in this study, along with its findings and recommendations, in order to create a baseline best-practice and/or model management policy for the oversight and accountability of DSTs in law enforcement.
- A typology of the harms associated with the misuse of DSTs by law enforcement should be developed.
- An explicit design process for developing and implementing DSTs by law enforcement should be developed. This approach should subsume the harm reducing protocols of SCP.
- A study explicitly focused on whether the increased use of advanced technologies and automation in law enforcement reduces the degree of direct human oversight and control over investigations and other critical police activities.

Appendix A: Dictation worksheets

Illustration 24:Dictation worksheet

Incident Information

1.) Initial or Supplemental	2.) CFS # (C/N)	3.) Date Occurred	4.) Time Occurred
5.) Through Date	6.) Through Time	7.) Date Reported	8.) Time Reported
9.) Refer to (e.g. Youth Div)	10.) Incident Code	11.) Shift	12.) Primary Ofc. Badge #
13.) Reporting Ofc Badge #	14.) Car # (A71)	15.) Street # & St. Name	16.) Building #
17.) Apartment #	18.) Disposition (see codes)	19.) Disposition Date	

BIAS CODES:

11 – Anti White	12 – Anti Black	13 – Anti American Indian
14 – Anti Asian	15 – Anti – Multi Racial	21 – Anti Jewish
22 – Anti Catholic	23 – Anti Protestant	24 – Anti Islamic
25 - Anti Other Religion	26 – Anti Multi Religion	27 – Anti Atheism
31 – Anti Arab	32 – Anti Hispanic	33 – Anti Other Ethnicity
43 – Anti Homosexual	44 – Anti Heterosexual	45 – Anti Sexual

Disposition Codes:

AA – Adult Arrest
AC – Active
IN – Inactive
JC – Juvenile Custody
UN – Unfounded
WP – Warrant Pending

Offense Information

20.) Incident Code	21.) Attempted / Completed	22.) Bias Code	23.) Location Code: *(see below)*
24.) # of Premises	25.) Force Y/N	26.) Gang Y/N	27.) Family Violence Y/N
28.) Criminal Activity *(see below)*	29.) Offender Suspected of Using (DICTATE TYPE OF DRUG)	30.) Weapon / Force *(see below)*	

Location Codes:

01 – Air / Bus / Train Terminal	09 – Drug Store / Dr. Office / Hospital	17 – Liquor Store
02 – Bank / Savings & Loan	10 – Field / Woods	18 - Parking Lot
03 – Bar / Night Club	11 – Government / Public Building	19 – Rental/Storage Facility
04 – Church / Synagogue	12 - Grocery / Supermarket	20 – Residence / Home
05 – Commercial / Office Bldg.	13 – Highway / Road / Alley	22 – School / College
06 - Construction Site	14 – Hotel / Motel / ect.	23 – Service / Gas Station
07 - Convenience Store	15 – Jail / Prison	24 – Specialty Store
08 – Department / Discount Store	16 – Lake Waterway	25 - Unknown

Criminal Activity Type:

B-Buying
C-Cultivating
D-Distributing/Selling
E-Exploiting Children
O-Operating / Promoting / Assisting
P-Possessing/ Concealing
T-Transporting / Transmitting / Importing
U- Using / Consuming

Weapon / Force Codes:

11 - Firearm	12 – Handgun	13 – Rifle	14 – Shotgun	15 – Other firearm	20 – Knife
30 – Blunt Object	35 – Motor Veh.	40 – Hands / Fist ect.	50 – Poison	60 – Explosives	65 – Fire
70 – Narcotics	90 – Other	95 – Unknown	99 - None		

Personal Information

31.) Type	32.) Involvement Status	33.) Name	34.) Sex	35.) D.O.B.	36.) Race	37.) H Y/N	38.) Address Street #, Street Name, Apt, City	39.) Tel. Number

Name Types:

I – Individual	B - Business	F – Financial
G – Government	R – Religious	S – Society
O – Other	U - Unknown	

Status Codes:

A – Arrestee	C – Complainant	D – Driver	AL- Alais
O - Offender	H – Other	P – Police	DN- Dangerous
S – Suspect	T – Turn over to	W – Witness	
V – Victim	J – Juvenile	M- Missing	

40.) Victim / Offender Code	41.) Injury Code

Victim / Offender Types:

SE- Spouse	GP – Grandparent	SS – Step Sibling	BE – Baby Sitter
EE – Employee	CS – Common Law Spouse	GC – Grand Child	OF – Other Family
BG – Boy / Girlfriend	ER – Employer	RU – Unknown	PA – Parent
IL – In Law	AQ – Acquaintance	CF – Child of BF or GF	SB – Sibling
SP – Step Parent	OK – Otherwise Known	FR – Friend	ST – Stranger
SC – Step Child	HH – Homosexual Relation	NE – Neighbor	XS – X-Spouse
VO – Victim was Offender		CH – Child	
EX – Ex-Live in/ Common Law			

Injury Type Codes:

N – None
I – Internal
M – Minor
T – Loss of Teeth
B – Broken Bones
L – Severe Laceration
O – Major
U - Unconscious

Vehicle Info

41.) Relationship	42.) License State	43.) License Number	44.) License Year
45.) Year of Vehicle	46.) Make	47.) Model	48.) Style (e.g. 2 door)
49.) Color	50.) Value	51.) VIN	52.) Damage Area
53.) Insurance Policy #	54.) Insurance Exp. Date	55.) Ins. Co. Name	56.) Ins. Co. Address

Vehicle Relationships

Abandoned Stolen / Lost Plate Citation Issued
Taken W/ O owners Permission Accident Vandalized Stolen Get away Car Undefined

Property Info

57.) Type Loss	58.) Description	59.) Value	60.) Quantity	61.) Reported Date	62.) NCIC Enter Date
63.) NCIC Cancel DT	64.) Owner	65.) Officer #	66.) NCIC	67.) SIN	68.) OAN
69.) Serial #	70.) Brand	71.) Model	72.) Mfg.		

Loss Codes:

B – Burned I – Impounded / Found ST–Stolen C – Counterfeited / Forged K – Safekeeping
D – Damaged/ destroyed L – Lost U – Unknown E – Evidence
N – None V – Vandalized F – Found R – Recovered SE-Seized

Narrati

73.) Report Date	74.) Report Time	75.) Badge Number	76.) Supervisors Name

Dictate Narrative

Incident Codes

0100 - HOMOCIDE
0101 – MURDER
0102 – MISCONDUCT W/ MV
0151 – SUICIDE
0152 – ATTEMPTED SUICIDE
0154 – SUDDEN DEATH
0200 – SEXUAL ASSAULT
0201 – SEXUAL ASSAULT
0206 – ATTEMPTED SEX ASSAULT
0300 – ROBBERY
0301 – ROBBERY COMMERCIAL
0304 – ROBBERY NON-COMMERCIAL
0308 – STREET ROBBERY
0311 – ATTEMPTED ROBBERY
0400 – ASSAULT AGGRAVATED
0401 – ASSAULT W/ INTENT TO KILL
0403 – ASSAULT W/ FIREARM
0404 – ASSAULT W/ DANG. WEAPON
0500 – BURGLARY
0501 – RESIDENCE
0507 – NON RESIDENCE
0516 – MANUF. / POSS OF BURG TOOLS
0600 – LARCENY NON AUTO
0601 – THEFT – SHOPLIFTING
0602 - THEFT – RESIDENCE
0603 – THEFT – NON RESIDENCE
0605 – THEFT FROM AUTO
0616 – ATTEMPTED THEFT
0700 – MOTOR VEHICLE THEFT
0701 – THEFT OF M.V.
0702 – RECOVERED M.V.
0703 – THEFT OF PLATE
0707 – USING W/O PERMISSION
0800 – ASSAULT OTHER
0801 – ASSAULT A POLICE / FIRE
0803 – RISK OF INJURY TO CHILD
0804 – STUDENT / TEACHER ASSAULT
0805 – SIMPLE ASSAULT
0806 – THREATENING
0807 – RECKLESS ENDANG
0808 – FIGHT
0810 – BOMB SCARE
0811 – ATTEMPT. ASSAULT
0850 – BREACH
0851 – DISORDERLY
0852 – HARRASSMENT
0860 – DISPUTE NO DISTURB.
0900 – ARSON / RECK BURNING
0901 – ARSON
0903 – ATTEMPT. ARSON
0904 – RECKLESS BURNING
1002 – FORGERY – ALL
1100 – FRAUD
1102 – FRAUD W/ CREDIT CARD
1105 – EXTORTION
1106 – THEFT OF SERVICE
1107 – ISSUING BAD CHECK
1200 – EMBEZZLEMENT
1300 – STOLEN / LOST PROPERTY
1301 – RECEIVING STOLEN PROPERTY
1302 – LOST PROPERTY
1303 – FOUND PROPERTY
1304 – RECOVERED PROPERTY
1306 – MYSTEROUS LOSS OF $$
1400 – VANDALISM
1401 – CRIM MISCH, PUBLIC PROP.
1402 – CRIM MISCH, PRIVATE PROP
1404 – WINDOW BREAKING
1500 – WEAPONS
1501 – CARRY A CONCEALED WEAP
1503 – ILL. POSS OF A WEAPON
1511 – CARRY WEAPON IN MV
1513 – UNLAWFUL DISCHARGE
1600 – PROSTITUTION
1602 – PATRONIZING A PROSTITUTE
1603 – PROSTITUTION
1604 – PERMITTING PROSTITUTION
1700 – SEX OFFENSES
1712 – PUBLIC INDENCY/EXPOSURE
1718 – VOYERISM
1800 – NARCOTICS
1801 – POSS. OF DRUGS
1802 – SALE OF DRUGS
1807 – MFG. OF DRUGS
1810 – CULTIVATION
1814 – PRESRIPT. FORGERY
1815 – POSS OF PARA
2000 – FAMILY AND CHILDREN
2004 – NEGLECT / ABUSE CHILD
2005 – FAM DISPUTE –ARGUMENT
2006 - FAM DISPUTE – VIOLENCE
2007 – FAM DISPUTE – ASSAULT
2101 – DWI
2210 – LIQUOR LAWS
2600 – ALL OTHER
2601 – ANIMAL NUISANCE
2602 – ANIMAL BITE
2603 – CRIM TRESPASS
2604 – FIRE WORKS
2608 – ABANDON M.V.
2609 – LITTERING
2610 – OTHER NUISANCE
2611 – DRUG OVERDOSE
2612 – MENTAL CASES
2618 – NON- M.V. ACCIDENT
2620 – BOATING VIO
2621 – BUILDING FOUND OPEN
2623 – MINOR JUVENILE COMPL.
2625 - NOTIFICATION.
2634 – OTHER MISC.
2800 – LOITERING
2802 – LOITERING
2809 – PROWLER
2810 – SUSP. PERSON
2900 – WANTED / MISSING PERSONS
2901 – MISSING CHILD
2903 – MISSING ADULT
2906 – LOCATED CHILD
2908 – LOCATD ADULT
2916 - RUNAWAY
2951 – WANTED PERSON /OTHER TOWN
3000 – TRAFFIC & M.V.VIO'S
3001 – MOVING VEHICLE
3002 – PARKED VEHICLE
3003 – EVADING RESPONS.
3004 – MVA FATAL
3005 – MVA NON-FATAL
3006 – MVA PROPERTY DAM
3007 – MVA PRIVATE PROP
3008 - RADAR
3009 – SUSPICIOUS M.V.
3010 – LIC. & REG. CHECK
3200 – ELECTION LAWS
3201 – ALL VIO'S
3900 - ESCAPES
3902 – ESCAPE FROM CUST
4000 – BLKMAIL/E XTORTION
4301 - BRIBERY
4303 – ATTEMPT. BRIBERY
4400 – OBSTRUCT JUSTICE
4401 - INTERFERING W/ OFC
4405 – FALSE REPORT OF INCD.
4500 - KIDNAPPING
4501 - KIDNAPPING
4502 – ATTEMPT. KIDNAP
4503 – UNLFL RESTRAINT
4504 – CUST. INTERFERRENCE
4700 - COUNTERFIETING
4701 – FORGERY / COUNTERFIETING
4800 – INTERNAL CODES
4801 – ASST. OTHER TOWN
4813 – SUPP INVESTIGATION
4850 – WARRANT SVC.
4854 – MEDICAL ASST.
4855 – BURG. ALARM

Bibliography

Abadie, A., & Gardeazabal, J. (2003). The Economic Costs of Conflict: A Case Study of the Basque Country. *American Economic Review, 93*(1).

Adler, P. A., & Adler, P. (2000). Observational Techniques. In N. K. Denzin & Y. S. Lincoln (Eds.), *Handbook of qualitative research* (2nd ed., pp. xx, 1065 , [1057] p.). Thousand Oaks, Calif.: Sage Publications.

Altimari, D. (2006). Slain Officer's Family Files Suit, Also Eyeing Action Against State Police. *Connecticut State Police Academy Alumni Association Website*. Retrieved from http://www.cspaaa.com/News/newsView.asp?NewsID=598

Arizona v. Evans, 514 1 (U.S. 1995).

Atkinson, P., & Hammersley, M. (2000). Ethnography and participant observation. In N. K. Denzin & Y. S. Lincoln (Eds.), *Handbook of qualitative research* (2nd ed., pp. xx, 1065 , [1057] p.). Thousand Oaks, Calif.: Sage Publications.

Auditor Of The Commonwealth (2009). *Office Of The State Auditor's Report On Information Technology Controls At The Criminal History Systems Board*: Commonwealth of Massachusettes Office Of The State Auditor.

Ball, K., & Webster, F. (2003). *The Intensification of surveillance : crime, terrorism and warfare in the information age* (1st ed.). London ; Sterling, VA: Pluto Press.

Beirne, P. (2005). *The Chicago school of criminology 1914-1945*. New York: Routledge.

Bernard, H. R. (2006). *Research methods in anthropology : qualitative and quantitative approaches* (4th ed.). Lanham, MD: AltaMira Press.

Brewer, J. D. (2000). *Ethnography*. Buckingham ; Philadelphia, PA: Open University Press.

Clarke, R. (1980). SituationalCrime Prevention: Theory and Practice. *British Journal of Criminology, 20*.

Clarke, R. (1997). *Situational crime prevention : successful case studies* (2nd ed.). Guilderland, N.Y.: Harrow and Heston.

Clarke, R., & Eck, J. (2006). *Crime Analysis for Problem Solvers In 60 Small Steps*. Washington DC: USDoJ, Office of Community Oriented Policing Services (COPS).

Clarke, R., & Eck, J. E. (2006). *Crime Analysis for Problem Solvers In 60 Small Steps*. Washington DC: USDoJ, Office of Community Oriented Policing Services (COPS).

Clarke, R., & Mayhew, P. (1980). *Designing out Crime*. London: H.M.S.O.

Clarke, R., & Newman, G. R. (2006). *Outsmarting the terrorists*. Westport, Conn.: Praeger Security International.

Cohen, L., & Felson, M. (1979). Social Change and Crime Rate Trends:A Routine Activity Approach. *American Sociological Review*.

Cohen, S. (1985). *Visions of social control : crime, punishment, and classification*. Oxford, UK: Polity Press.

Creswell, J. W. (2007). *Qualitative inquiry & research design : choosing among five approaches* (2nd ed.). Thousand Oaks: Sage Publications.

Deleuze, G., & Guattari, F. (1987). *A thousand plateaus : capitalism and schizophrenia*. Minneapolis: University of Minnesota Press.

Denzin, N. K. (1989). *The research act : a theoretical introduction to sociological methods* (3rd ed.). Englewood Cliffs, N.J.: Prentice Hall.

Denzin, N. K., & Lincoln, Y. S. (2008). *Strategies of qualitative inquiry* (3rd ed.). Los Angeles: Sage Publications.

Eck, J. E., & Spelman, W. (1987). Who Ya Gonna Call? The Police as Problem-Busters. *Crime and Delinquency, 33*(1).

Emsley, C., & Shpayer-Makov, H. (2006). *Police detectives in history, 1750-1950*. Aldershot, Hants, England ; Burlington, VT: Ashgate.

Ericson, R. V., & Haggerty, K. D. (1997). *Policing the risk society*. Toronto ; Buffalo: University of Toronto Press.

Farmer, D., & Mann, C. C. (2003). Part one: Surveillance Nation. *Technology Review, 106*(3).

Feeley, M. (1979). *The process is the punishment : handling cases in a lower criminal court*. New York: Russell Sage Foundation.

Fontana, A., & Frey, J. H. (2000). Interviewing: The art of science. In N. K. Denzin & Y. S. Lincoln (Eds.), *Handbook of qualitative research* (2nd ed., pp. xx, 1065 , [1057] p.). Thousand Oaks, Calif.: Sage Publications.

Frankfort-Nachmias, C., & Nachmias, D. (2008). *Research methods in the social sciences* (7th ed.). New York, NY: Worth Publishers.

Friedman, B. (1997). *Human values and the design of computer technology*. Stanford, Calif. Cambridge ; New York: CSLI Publications ;
Cambridge University Press.

Fussell, J. (2001). *Group Classification on National ID Cards as a Factor in Genocide and Ethnic Cleansing*. Paper presented at the International Association of Genocide Scholars Conference. from http://www.preventgenocide.org/prevent/removing-facilitating-factors/IDcards/

Gandy, O. H. (1993). *The panoptic sort : a political economy of personal information*. Boulder, Colo.: Westview.

Garfinkel, S. (2001). *Database nation : the death of privacy in the 21st century*. Cambridge, Mass.: O'Reilly.

Garland, D. (2001). *The culture of control : crime and social order in contemporary society*. Chicago: University of Chicago Press.

Georgia Tech Information Security Center (2008). *Emerging Cyber Threats Report for 2009, Data, Mobility and Questions of Responsibility will*

Drive Cyber Threats in 2009 and Beyond: Georgia Tech University.

Gerring, J. (2007). *Case study research : principles and practices*. New York: Cambridge University Press.

Glaser, B. G., & Strauss, A. L. (1968). *The discovery of grounded theory: strategies for qualitative research*. London,: Weidenfeld and Nicolson.

Goldsmith, A. J., & Lewis, C. (2000). *Civilian oversight of policing : governance, democracy, and human rights*. Oxford ; Portland, Or.: Hart Pub.

Goldstein, H. (1979). Improving Policing: A Problem Oriented Approach. *Crime and Delinquency, 25*(April).

Goldstein, H. (1990). *Problem-oriented policing*. Philadelphia: Temple University Press.

Goold, B. J. (2003). Public Area Surveillance and Police Work: the impact of CCTV on police behaviour and autonomy. *Surveillance and Society, 1*(2).

Goold, B. J. (2004). *CCTV and policing : public area surveillance and police practices in Britain*. Oxford ; New York: Oxford University Press.

Gorden, R. L. (1980). *Interviewing : strategy, techniques, and tactics* (3d ed.). Homewood, Ill.: Dorsey Press.

Greenfield, A. (2006). *Everyware : the dawning age of ubiquitous computing*. Berkeley, CA: New Riders.

Grossman, R. (2001). *Data mining for scientific and engineering applications*. Dordrecht ; Boston, Mass.: Kluwer Academic.

Guba, E. G., & Lincoln, Y. S. (1981). *Effective evaluation* (1st ed.). San Francisco: Jossey-Bass Publishers.

Haggerty, K., & Ericson, R. (2000). The Surveillant Assemblage. *British Journal of Sociology, 51*(4).

Herring v. United States, 555 513 (US 2009).

Inspector General (2005). *The Federal Bureau Of Investigation's Management Of The Trilogy Information Technology Modernization Project*: U. S. Department of Justice Office of the Inspector General, Audit Division.

Inspector General (2006). *Federal Agencies' Efforts to Protect Sensitive Information, A Report to the Office of Management and Budget. PCIE/ECIE Report compiled by the PCIE Information Technology Roundtable and the Federal Audit Executive Council Information Technology Committee*: US Department of Education.

Inspector General (2007). *A Review of the Federal Bureau of Investigation's Use of National Security Letters*: U. S. Department of Justice Office of the Inspector General.

Krippendorf, K. (2004). *Content Analysis: An Introduction to Its Methodology* (2ed. ed.). Thousand Oaks: Sage Publications.

Lambert, E. Y. (1990). *The Collection and interpretation of data from hidden populations*. Rockville, MD (5600 Fishers Lane, Rockville 20857)
Washington, D.C.: U.S. Dept. of Health and Human Services, Public Health Service, Alcohol, Drug Abuse, and Mental Health Administration
For sale by the Supt. of Docs., U.S. G.P.O.

Laurant, C. (Ed.). (2003). *Privacy and Human Rights An International Survey of Privacy Laws and Developments*. Washington D.C., London: Electronic Privacy Information Center; Privacy International.

Lee, R. M. (1995). *Dangerous fieldwork*. Thousand Oaks, Calif.: Sage Publications.

Los, M. (2004). The Technologies of Total Domination. *Surveillance and Society, 2*(1).

Lyon, D. (1994). *The electronic eye : the rise of surveillance society*. Minneapolis: University of Minnesota Press.

Lyon, D. (2002). *Surveillance society : monitoring everyday life*. Buckingham [England] ; Philadelphia: Open University Press.

Lyon, D. (2003a). *Surveillance after September 11*. Malden, Mass.: Polity Press in association with Blackwell Pub. Inc.

Lyon, D. (2003b). *Surveillance as social sorting : privacy, risk, and digital discrimination*. London ; New York: Routledge.

Lyon, D. (2007a). *Surveillance studies : an overview*. Cambridge, UK ; Malden, MA: Polity.

Lyon, D. (2007b). Surveillance, power and everyday life. In R. Mansell (Ed.), *The Oxford handbook of information and communication technologies*. Oxford ; New York: Oxford University Press.

Marx, G. T. (1988). *Undercover : police surveillance in America*. Berkeley: University of California Press.

Marx, G. T. (1992a). Let's Eavesdrop On Managers *Computerworld*.

Marx, G. T. (1992b). When the Guards Guard Themselves: Undercover Tactics Turned Inward *Policing and Society, 2*.

Marx, G. T. (2002). What's New About the "New Surveillance"? Classifying for change and continuity. *Surveillance and Society, 1*(1).

Mayhew, P., Clarke, R. V., Hough, M., & Sturman, A. (1976). *Crime as Opportunity*. London: H.M.S.O.

Merton, R., & Kendal, P. (1946). The Focused Interview. *American Journal of Sociology, 51*.

Monahan, T. (Ed.). (2006). *Surveillance and security : technological politics and power in everyday life*. New York: Routledge.

Moscaritolo, A. (2009). Mass. police snooped on celebrities' records. *Security Professional Magazine*. Retrieved from http://www.scmagazineus.com/Mass-police-snooped-on-celebrities-records/article/136288/

Müller, C., & Boos, D. (2004). Zurich Main Railway Station: A Typology of Public CCTV Systems. *Surveillance and Society, 2*(2/3).

National Institute of Justice (2009). *High-Priority Criminal Justice Technology Needs*. Washington, D.C.: Office of Justice Programs

Neuendorf, K. (2002). *The Content Analysis Handbook*. Thousand Oaks: Sage Publications.

Newman, G. R., & Clarke, R. (2003). *Superhighway robbery : preventing e-commerce crime*. Cullompton: Willan.

Newman, O. (1972). *Defensible space; crime prevention through urban design*. New York,: Macmillan.

Norris, C., McCahill, M., & Wood, D. (2004). The Growth of CCTV: a global perspective on the international diffusion of video surveillance in publicly accessible space. *Surveillance and Society, 2*(2/3).

O'Harrow, R. (2005). *No place to hide*. New York: Free Press.

Parenti, C. (2003). *The soft cage : surveillance in America : from slavery to the war on terror*. New York: Basic Books.

Patton, M. Q. (2002). *Qualitative research and evaluation methods* (3 ed.). Thousand Oaks, Calif.: Sage Publications.

Power, S. (2002). *A problem from hell : America and the age of genocide*. New York: Basic Books.

Rhodes, L. A. (2004). *Total confinement : madness and reason in the maximum security prison*. Berkeley, Calif.: University of California Press.

Ruegg, J., November, V., & Klauser, F. (2004). CCTV, Risk Management and Regulation Mechanisms in Publicly-Used Places: a Discussion Based on Swiss Examples. *Surveillance and Society, 2*(2/3).

Rule, J. B. (1974). *Private lives and public surveillance; social control in the computer age*. New York,: Schocken Books.

Rule, J. B. (2007). *Privacy in peril*. Oxford ; New York: Oxford University Press.

Sætnan, A. R., Lomell, H. M., & Wiecek, C. (2004). Controlling CCTV in Public Spaces: Is Privacy the (Only) Issue? Reflections on Norwegian and Danish Observations. *Surveillance and Society, 2*(2/3).

Scholz, R. W., & Tietje, O. (2002). *Embedded case study methods : integrating quantitative and qualitative knowledge*. Thousand Oaks, Calif.: Sage Publications.

Seifert, J. W. (2004). *Data Mining: An Overview, CRS Report for Congress RL31798*: Congressional Research Service, The Library of Congress.

Shaw, I., & Gould, N. (2001). *Qualitative research in social work*. London: Sage.

Singleton, R., & Straits, B. C. (2005). *Approaches to social research* (4th ed.). New York: Oxford University Press.

Sparrow, M. K. (1994). *Imposing duties : government's changing approach to compliance*. Westport, Conn.: Praeger.

Sparrow, M. K. (2008). *The character of harms : operational challenges in control*. Cambridge ; New York: Cambridge University Press.

Sparrow, M. K., Moore, M. H., & Kennedy, D. M. (1990). *Beyond 911 : a new era for policing*. [New York, N.Y.]: Basic Books.

Spradley, J. P. (1979). *The ethnographic interview*. New York: Holt, Rinehart and Winston.

Stake, R. E. (1995). *The art of case study research*. Thousand Oaks: Sage Publications.

Stanley, J. (2004). *The Surveillance-Industrial Complex: How the American Government Is Conscripting Businesses and Individuals in the Construction of a Surveillance Society*: ACLU.

Stanley, J., & Steinhardt, B. (2003). *Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society*: ACLU.

Steinhardt, B. (2007). Active Millimeter Wave, New Airport Body Scanners Troubling to ACLU Privacy Expert Retrieved Sep 9, 2008, from http://www.mindfully.org/Technology/2007/Active-Millimeter-Wave11oct07.htm

Survey Research Center (1976). *Interviewer's manual* (Rev. ed.). Ann Arbor: Survey Research Center, Institute for Social Research, University of Michigan.

Sutton, A., & Wilson, D. (2004). Open-Street CCTV in Australia: The Politics of Resistance and Expansion. *Surveillance and Society, 2*(2/3).

TAPAC (2004). *Safeguarding Privacy in the Fight Against Terrorism: The Report of the Technology and Privacy Advisory Committee [TAPAC]*.

Technology And Privacy Advisory Committee (2004). *Safeguarding Privacy In The Fight Against Terrorism The Report Of The Technology And Privacy Advisory Committee*: US Department of Defense.

Tellis, W. (1997). Introduction to Case Study. *The Qualitative Report, 3*(2).

Tewksbury, R. A., & Mustaine, E. E. (2004). *Controversies in criminal justice research*. [Cincinnati, OH]: Anderson Pub.

Thompson, F. (2000). Of Mouse and Management- Improving Federal Performance for the 21st Century. *Journal of Public Inquiry*(Fall/Winter).

Trotter, R. T. (1999). Friends, relatives, and relevant others: Conducting ethnogrpahic network studies. In J. J. Schensul (Ed.), *Mapping social networks, spatial data & hidden populations* (pp. xv, 205 p.). Walnut Creek, Calif.: AltaMira Press.

Wakefield, A. (2004). The Public Surveillance Functions of Private Security. *Surveillance and Society, 2*(4).

Walby, K. (2006). Little England? The rise of open-street Closed-Circuit Television surveillance in Canada. *Surveillance and Society, 4*(1/2).

Webb, M. (2006). *Illusions of security : global surveillance and democracy in the post-9/11 world* (1st ed.). San Francisco, USA: City Lights Books.

Weppner, R. S. (1977). *Street ethnography : selected studies of crime and drug use in natural settings*. Beverly Hills, Calif.: Sage Publications.

Werner, O., Schoepfle, G. M., & Ahern, J. (1987). *Systematic fieldwork*. Newbury Park, Calif.: Sage Publications.

Willison, R. (2008). Applying Situational Crime Prevention To The Information Systems Security Context. In M. M. McNally & G. R. Newman (Eds.), *Perspectives on identity theft, Crime prevention studies* (Vol. 23). Monsey, N.Y.: Criminal Justice Press.

Wilson v. City of Louisville, Ky (Jefferson County Cir. Ct. Nov. 11, 1998).

Winnett, R., & Swaine, J. (2008). Data on 130,000 criminals lost Retrieved Aug 22, 2008, from http://www.telegraph.co.uk/news/newstopics/politics/2601056/Data-on-130000-criminals-lost.html

WinterCorp (2007). Winter TopTen Programs Retrieved April 20, 2007, from http://www.wintercorp.com/VLDB/2005_TopTen_Survey/TopTenProgram.html

Wood, D. M. (2006). *A Report on the Surveillance Society [Full Report]*: [UK] Information Commissioner's Office.

Wortley, R. (2002). *Situational prison control : crime prevention in correctional institutions*. Cambridge, UK ; New York: Cambridge University Press.

Wright, S. (2005). The ECHELON Trail: an Illegal Vision. *Surveillance and Society, 3*(2).

Yin, R. K. (2009). *Case study research : design and methods* (4th ed.). Los Angeles: Sage Publications.

Zurawski, N. (2004). "I Know Where You Live!" – Aspects of Watching, Surveillance and Social Control in a Conflict Zone (Northern Ireland). *Surveillance and Society, 2*(4).

Zureik, E., & Salter, M. B. (2005). *Global surveillance and policing : borders, security, identity*. Cullompton ; Portland, Ore.: Willan.