



Homeland Security: 2015

Proceedings of the Futures Working Group

Volume 2



Homeland Security, 2015:
A Series of Working Papers from the Futures Working Group

Editor:
Michael Buerger
March, 2006

Acknowledgments

The Futures Working Group would like to express our thanks and gratitude to the University of Phoenix for hosting the April 2005 meeting. In particular, our thanks to Bill Pepicello, Provost; Tom Lemen, Dean, College of Arts and Sciences; Gil Linne, Dean, College of Health and Human Services; Franzi Walsh, Assistant Dean, College of Health and Human Services; and Rob Olding, Associate Dean, College of Health and Human Services. Thanks also the FWG member Al Youngs, a member of the University of Phoenix faculty, who helped arrange the meeting. Also, thanks to Stephanie Kennerley and John Jarvis for editing the final version.

Special thanks to John Smart, President of the Institute for the Study of Accelerating Change, whose presence at and contributions to the Phoenix meeting were exceptionally educational and inspirational.

Table of Contents

A Word from the Chairman

Carl J. Jensen III 7

Homeland Security in 2015

Bernard H. Levin and Carl J. Jensen III 9

Law Enforcement Technology 2015

Charles “Sid” Heal, Thomas Cowper, and Andreas Olligschlaeger 28

Policing and Homeland Security in 2015

Richard A. Myers and Alberto Melis 38

On the Horizon: Police Training in 2015

Joseph Schafer, Sandy Boyd, and Alan Youngs 62

Privacy 2015

Michael E. Buerger 64

Afterword

Michael E. Buerger 84

About the Authors 86



A Word from the Chairman

Since our first meeting at the FBI Academy in the winter of 2002, the Futures Working Group (FWG) has been going strong. In addition to several articles, numerous training and conference appearances, and two books, the group continues to probe the outer fringes of what futurists call “possible, probable, and preferable” futures.

The articles in the present volume were initiated at a FWG meeting hosted by the University of Phoenix, in the spring of 2005. During that gathering, we were privileged to have John Smart of the Acceleration Studies Foundation (<http://www.accelerating.org/>) share some of his thoughts about the future. We thank the University for its gracious hospitality and John for his stunning insights; nothing could have better prepared us for embarking upon this volume.

Given the state of the world and the policing profession in early 2005, we could not have imagined a more timely topic than that of homeland security. To be sure, much has been written about that subject; however, little has concerned itself with the future of homeland security and its nexus with policing. As our discussions progressed, it became clear that many possible futures exist with regard to this very important area. This volume is an attempt to consider some of them and, further, to articulate strategies to bring about the best of all possible futures.

As you read the articles contained herein, remember that the goal of futurists is to make others think. This is generally accomplished by introducing new, challenging, and at times disconcerting ideas. You may agree with some authors and disagree with others. You may even feel somewhat unnerved by what has been written. That is all to the good. As expressed in a prior volume: “Ultimately, it

is our fervent desire that this slim volume will motivate you to devise ways to create your own preferred futures—for yourself, your agency, and the communities you serve.”

That goal hasn’t changed. We hope you enjoy our efforts.

Carl J. Jensen III, Ph.D.
*Supervisory Special Agent
Behavioral Science Unit, FBI Academy
Chairman, Futures Working Group*

*Quantico, Virginia
December, 2005*

The opinions and statements contained in this volume are those of the individual authors and should not be considered an endorsement by the FBI or the Department of Justice for any policy, program, or service.



Homeland Security in 2015

Bernard H. Levin, Ed.D.

Carl J. Jensen III, Ph.D.

What Does/Will Homeland Security Mean

Reflecting upon the meaning of “homeland security” brings to mind Justice Stewart’s memorable pronouncement on obscenity:

“I shall not today attempt further to define the kinds of material I understand to be embraced... but I know it when I see it...”^{iv}

Most of us have an idea of what we mean when we refer to “homeland security.” The mission statement of the Department of Homeland Security (DHS) provides a benchmark:

“We will lead the unified national effort to secure America. We will prevent and deter terrorist attacks and protect against and respond to threats and hazards to the nation. We will ensure safe and secure borders, welcome lawful immigrants and visitors, and promote the free-flow of commerce.”^v

We suggest that both the definition and boundaries of that term will evolve as we approach the year 2015. Until a workable, universal definition emerges, however, we will find ourselves mired in confusion, generally allowing whatever tail happens to come along to wag an increasingly massive dog.

To be sure, terrorism is, and will likely continue to be, a major component of homeland security.

Nonetheless, as time goes on, we suspect that the definition will expand, especially if the United States is fortunate enough to be spared from

another major event similar to 9\11: the multiple attacks against targets in New York City and Washington, D.C. on September 11, 2001. The DHS mission statement cited above, even if it remains unchanged, is broad enough to include a wide range of threats: economic espionage, pandemics, natural disasters, environmental meltdown, crime (of both the sophisticated and street variety), and just about everything else even remotely connected to the stability of the United States.^{vi}

What is and what is not defined as being a component of “homeland security” will have a major impact on the police. For example, if street crime rises to the level of a threat to national security (and we suspect that the bar for defining something that way will decrease), don’t be surprised to see the military on the front lines (*see Scenario 1*).^{vii} In addition, resource allocation, particularly at the federal level, increasingly will be tied to the extent to which something serves to bolster the perceived security of the homeland.^{viii}

The police will be caught in the middle, constantly redefining their mission to “follow the money” or trying to take up the slack when federal agencies are deployed in other missions.

The Need for Change

The world of 2015 has the potential to be very different from the world of today. Futurists note that the rate of technological change is accelerating (Kurzweil, 1999) even as social change stagnates (Smart, 2003). One futurist has opined that by the year 2020, the amount of information in the world will double every 73 days (Schwartz 1999).

The following possible trends are provided, not as predictions, but as suggestions to promote thought. Readers are encouraged to consider how each may affect his/her agency:

- 1) The rise of states like China and India, who will challenge the United States and the West in terms of technical know-how, and who will demand an increasing share of the world's resources.
- 2) Migration to China, the United States, Europe, and Russia of individuals to meet the needs of the workforce in aging societies. Unless societies work hard not to make these folks feel marginalized, the migrants will be ripe for radicalization.^{xi}
- 3) Youth bulges in the Middle East & Africa (comparable to the "baby boom" in America), providing foot soldiers for terrorist and criminal groups. When combined with trend #2, this could prove to be a great challenge for policing.
- 4) Ubiquitous information technology (IT), allowing for true virtual communities rather than physical groups. Computers and chips will be small, inexpensive, and everywhere. There will be no such thing as computer crime: all crime with few exceptions, will involve some use of computers.
- 5) In a world where physical boundaries are becoming less important, people will increasingly define themselves by ethnicity, religion, economic class and belief-system as opposed to nationality. Smart (2005) notes that the drivers of change in the near future will be, in order of importance: technology, economics, and politics. The nation-state is not dead, but its stature continues to decline.
- 6) Groups with diverging interests (organized crime, terrorists) will work together in temporary alliances or "one-shot deals" when it suits their purpose.
- 7) Sadly, absent a paradigm shift, outlaw groups will negotiate the information age far more adroitly than the groups sworn to stop them.
- 8) Weapons of mass destruction will proliferate, even at the individual level. This will come about primarily as a result of increased access to information via the Internet (biological, chemical, and radiological devices are the most likely to emerge, nuclear less so).

One of the central themes of the Information Age is the empowerment of the individual and the small group. To that end, and given the above, one thing seems abundantly clear: the action is going to be at the street level. That means that, in terms of homeland security, local law enforcement will either be on the cutting edge or will become relegated to second-class citizenship.

Terrorism in 2015^{xii}

*The groundhog is like most other prophets;
it delivers its prediction and then disappears.*

Bill Vaughn

It's the end of the world as we know it.

REM

It is with some trepidation that we discuss what terrorism (or anything else, for that matter) will resemble in 2015. Nevertheless, there are certain themes that will infuse the next several years; these, in turn, will affect trends.^{xiii}

One element that ties many terrorist organizations together today is a general reaction against globalization. Each group would describe its concerns somewhat differently: al Qaeda decries the decadent influences of the West, the white supremacists rail against the internationalist/Jewish conspiracy, and the environmentalists deplore what they see as the borderless, economically-driven military-industrial complex. Each of these is a reaction against various elements of our increasingly tied-together world.

It is doubtful that globalization is going to go away; indeed, some describe it as the most pervasive influence on the first part of the 21st century (see, for example, Friedman (2000)). To that end, much like the Luddites of the 18th century, it is likely that extreme reactions against the "new world" will spawn many who see it as their duty to violently oppose ever-accelerating change.

Added to this, it is doubtful that the economic benefits of the Information Age will be evenly distributed (National Intelligence Council, 2004). A wide gap between the haves and have-nots, combined with a shrinking middle class, does not bode well for stability (Gurr, 1970).

Increasingly, it is likely that terrorist and criminal groups will develop temporary alliances when it suits their purpose. This is not a new phenomenon—in the 1970s and 1980s radical left-wing groups recruited felons to assist them in robbing banks. Likewise, in the 1980s the Libyan government contracted with the Japanese Red Army to carry out bombings in the United States.

Today, groups like the Revolutionary Armed Forces of Colombia engage in both terrorist and criminal activities. According to the U.S. Department of State:

The FARC has well-documented ties to the full range of narcotics trafficking activities, including taxation, cultivation, and distribution (U. S. Department of State, 2004).

Further, some future alliances may prove quite strange; consider the words of Aryan Nation's leader August Kreis, offering his support for al Qaeda:

You say they're terrorists, I say they're freedom fighters. And I want to instill the same jihadist feeling in our peoples' heart, in the Aryan race, that they have for their father, who they call Allah (Shuster, 2005)

Individual actors and small groups will be able to inflict greater levels of harm than in the past. Increased access to information combined with a "cyber sense of group" ^{xiv} translates to a very small investment needed for a very large effect (e.g., while not directly on point, consider the enormous psychological and economic impact the snipers of

2003 had on the Washington, D.C. environs).

Put succinctly, the potential for ever-increasing acts of terrorist violence seems more rather than less as we approach 2015. Former National Security Council (NSC) member Richard Clarke (2005) described several possible al Qaeda attack scenarios in a piece that he recently wrote for *The Atlantic Monthly*. His outline of potential targets in the United States included schools, shopping malls, and airliners; perhaps most alarming, each was based on intelligence Clarke had received while in office at the NSC.

As noted above, youth bulges in poor countries will likely drive migration to more affluent areas, including the United States. Some areas have lately noted an almost quantum leap in the number of recently arrived immigrants, many of whom do not speak English and do not understand U.S. culture. Police agencies, through outreach and training, can go a long way toward helping individuals and groups feel less marginalized (one step on the road to becoming a solid citizen rather than a criminal/terrorist). As well, good relations with a particular community make it more likely that members of that community will trust the police enough to provide information about possible terrorist or criminal enterprises in their midst.

Possible Specific Trends

Radical Islamic Movement: Since its ouster from Afghanistan, al Qaeda has become quite decentralized, with its leadership seemingly less involved in directing operations. Several smaller organizations may emerge, with figures like bin Laden looked to for spiritual and political inspiration. The nature of the Radical Islamic Movement in 2015 will depend to a great extent on political actions currently unfolding. For example, the manner in which the United States is perceived in predominantly Islamic countries (democratizing

force or occupier) will drive opinion.^{xv} As well, whether governments in the Middle East and Africa can effectively meet the needs (educational, economic, political, and religious) of the expected youth bulges will have a significant effect on this movement. That said, it is difficult to imagine that the Radical Islamic Movement will not be with us for some time to come; instead, a best-case scenario might be that it can be contained, with only sporadic and ineffective acts of violence.

Radical Animal Rights/Anarchist/Environmental Movements: At least four areas of concern to the animal rights/anarchist/environmental movement(s) are advancing, in some cases exponentially, to form a “perfect storm” for criminal activism: globalization, energy consumption, technology, and reports of environmental degradation.^{xvi} As well, the economic gap between the rich and the poor, predicted to widen, has always been a touchstone issue for these groups, especially as it is perceived to disproportionately affect indigenous peoples. To date, the tactics of the enviro/animal/anarchist movement(s) have not significantly advanced their interests; to that end, it is quite possible that we will witness more frequent and lethal attacks, primarily against property but increasingly against individual targets of interest (police, government/corporate officials, research facilities, etc.).

Hate Groups/Single Interest Groups/the New Luddites: Although some well-known groups have been in decline for years, individual arrests indicate that those who engage in criminal activity to advance supremacist ideologies still exist.^{xvii} Like other information age entities, the supremacy and hate movements have made the move from hierarchies to networks. Indeed, supremacist movements and hate groups may witness a renaissance, particularly if immigration levels rise as expected. Already, citizen vigilante groups patrol the

U.S.-Mexican border, often using more sophisticated tools than those available to the authorities. It is expected that new single interest groups will emerge as well. Concern about new technologies (e.g., nanotechnology and artificial intelligence) has provoked debate among scientists and engineers and has spawned Armageddon-like scenarios. It is not unforeseeable that a new Neo-Luddite,^{xviii} anti-technology movement may come to the fore; their interests, while more narrowly-focused, could easily overlap with those of the animal rights/anarchist/environmental movements.

In general, and of particular interest to the local police, the structures of each of the above may look quite similar—small, autonomous, flexible units that seek to fly under the radar of the authorities. Depending on their level of operational security, terrorists may be quite difficult to locate. And yet, complete invisibility will likely be impossible. All groups leak information from time to time. So one very important role for those involved in homeland security will be that of “leak detector.” The cop on the beat, with his/her intimate knowledge of the community, is in a prime position to do just that.

Crime in 2015

Because that’s where the money is.

Line allegedly spoken by Willie Sutton when asked why he robbed banks.

The world is shrinking. The legal system that most of us understand was developed at a time of specific jurisdictions, defined by articulated boundaries. That world is disappearing.

Increasingly, criminals are realizing that the real money is contained online, in ones and zeros. The more sophisticated ones will continually take advantage of that and will steal electronically rather than physically. And yet, bank robberies, burglaries

and the like will not disappear. Rather, they will be committed by those who lack the skills to hack, crack, and maraud.

The category termed “computer crime” may begin to vanish—it seems likely that most crimes, with some exceptions, will involve the use of computers. The rather crude cyber-scams of today will likely increasingly become replaced by ever more sophisticated operations. The authors envision a high-speed cat-and-mouse game, in which criminals attempt to stay one step ahead of authorities, evading and plundering as the police ratchet up detection and target hardening (see *Scenario 2* for one possible future of cyber-crime fighting).

Policing is at a crossroads—it will always have to go after the low hanging fruit (the “dumb” criminals who engage in high profile events and who are relatively easy to catch). The tricky part will be the extent to which agencies, particularly local agencies, engage those involved in serious, sophisticated (but somewhat less publicized) crime. Only doing the former means to retain, for the most part, the status quo. To pursue the latter requires an investment in personnel and training, and a re-evaluation of the meaning of “policing.” If the police are unwilling or unable to confront sophisticated criminals, that void will be filled by someone else (e.g., the private sector).

Defining Homeland Security: The Maintenance of Multi-System Stability

In order to better understand what homeland security in the year 2015 **should** mean, we note that its current understanding is fundamentally incompatible with the information age, specifically

with regard to virtual life and permeable borders. Instead, we propose that homeland security be viewed as the maintenance of multi-system stability.

The systems we believe to be significant components of homeland security include:

- Physical Infrastructure** (e.g., water and sewage, energy, roads, waste management)
- Virtual Infrastructure** (e.g., communication networking, including but not limited to the Internet, cable, cellular, satellite and more traditional telephony)
- Social Infrastructure** (relationships between social groups as well as between social groups and government)

In each case, security translates as system stability, and thus predictability of the environment in which we operate. It may seem that this definition is not without weaknesses. For example, some may feel that it implies or endorses resistance to change. However, the contrary is true. It is the existing construct of homeland security that implies—indeed, requires—resistance to change.

The new definition focuses not only on government, but also on individuals, social groups, and private sector players as process drivers. While stability of governmental services—especially infrastructure—is necessary, the key points of mensuration are at the level of the individual service recipient.

Is the distinction we are trying to draw merely straining at a gnat or drawing a distinction without a difference? No. By buying into the proposed definition, we can abandon the industrial-age trappings of the current model. “Border Patrol” yields to “Systems Evolution and Applications Protection” (SEAP). The former implies that we must play defensive ball. The proposed definition implies active, dynamic, and recipient-focused

activities.

An analogy is that of two approaches to reducing damage done by hackers. One general approach develops a list of signatures against which to check incoming files. That approach is historical and defensive. It results in “acceptable” losses. It cannot anticipate. The other general approach looks at stabilizing files and file behavior. In this latter approach one sees terms such as “immunizing” and “self-repairing.”

If we take a SEAP approach, we can look toward future needs rather than historical threats. We can foment system evolution rather than simply respond to breaches and system failures. The primary reason SEAP will be able to do so and the present system cannot is that the center of SEAP is the end user.

Implications of this change in process are significant. For example, discussions of system down-time, outcomes assessment, reliability, and goodness of fit become possible. Instead of our present focus on boundaries, where we assume that somehow we can make the boundaries impermeable, we focus on the stability of systems and services provided to citizens and other eligible individuals and groups. The focus becomes predictability, rather than boundaries.

Does Homeland Security Differ from Crime Prevention?

Construed as SEAP, homeland security becomes a superset of crime prevention. Traditional crime prevention suffers from an unavoidable problem—the inability to measure that which did

not happen. One cannot measure negative events. SEAP, on the other hand, is an approach that does not require separate treatment of crime and allows positive measurement of outcomes. Consider, e.g., re-thinking safety as “days since a lost-time injury” versus “number of crashes so far this year.” The distinction is non-trivial.

There are distinct advantages to constructing both the current homeland security and traditional crime measures under a common rubric with a common set of procedures and common outcome measures. Efficiencies abound because redundant hierarchies become irrelevant. Effectiveness may also increase. For example, by use of a common rubric, barriers to information flow may be removed. “Special” processes for homeland security and crime prevention would become harder to defend.

The focus of SEAP on outcomes also has the advantage of fomenting transparency. Transparency lives best when the measures do not require special knowledge to understand. The general public will understand when “system up-time” is used across many dimensions. That concept remains the same across multiple dimensions, multiple systems, and multiple contexts. Crime prevention, on the other hand, has never been presented (and probably cannot be presented) in a way that leads the average citizen to understand whether it works or not. Consider how difficult it is to get across even the simple notions that larcenies are more frequent than violent crimes, and that for most purposes random patrol accomplishes little and what makes headlines is rarely what kills us. If we cannot get these notions across, then we cannot successfully communicate with those we serve and we wind up with built-in inefficiencies. In effect, through poor design we create resource-poor systems, systems designed to fail.

External/Homeland Security

threats metamorphose faster than other crime?

Perceived rates of change depend on perceptions of scale and on contexts. Crime appears to change slowly because the rules that create crime (law) change only annually or biennially or via case law—very slow processes indeed. Homeland security threats appear to metamorphose quickly because we perceive the whole problem as relatively new, we are still exploring its dimensions, the definition is unstable, and consensus is lacking on some of what we call homeland security. However, these perceived differences in rate of change are illusory.

Both homeland security and crime are characterized by deviations from prescribed behavior. In both domains, part is of concern to the general public (e.g., street crime and employment of illegal immigrants) while part is of little or no concern to the general public (e.g., insider trading and intellectual property smuggling). The general public sees street crime and is unhappy. Most homeland security issues are not visible to the general public and, except for perceived threats to safety and jobs, there is little intrinsic interest in it. The general public can accurately describe the injury created by street crime. The general public cannot accurately describe the injury created by an overstayed visa or by violation of a software license. More important, how can we coherently and persuasively argue which category contains industrial espionage? Street-corner drug sales? Identity theft? The fact of the matter is that crime overlaps significantly with homeland security, that crime is one means to breach homeland security, and that breaches of homeland security may foment crime (cf. MS-13 players moving between Salvador and the U.S. depending on which government is most diligently looking for them at the moment). The separation of the two constructs in our globalized world impedes success in both. Thus, system stability serves as both a goal and a

common means of understanding homeland security and crime.

Industrial Age Bureaucracies & SEAP

Governments have, as their *raison d'être*, the protection of their citizens from threat. Yet the manner in which this plays out can vary considerably from government to government. Consider an extreme example from the industrial age, the factory town: In addition to the factory itself, the company ran stores, schools, hospitals and other services from the cradle to the grave (or, at least, the cradle-to-retirement). The factory billed itself as a benevolent patriarch, capable and willing to support its employees in all facets of their lives. Implicit in this was the notion that, not only was the company able to care for its employees, it was **better** able to care for them than the employees themselves. Think benevolent caretaker vs. individual actor.

Industrial age bureaucracies act similarly to factory towns, setting themselves up as wise and capable patriarchs. As the protector of the people, it is in the interest of a bureaucratic government to increase threat—or at least the perception of threat—so that citizens fear more and thus are willing to give up more of their resources, both in terms of finances and freedoms. The performance of bureaucratic institutions is often resistant to mensuration, both because the patriarch often does not willingly invite oversight and because measurement in areas such as “prevention” can be plain difficult. Holding government accountable, under the current conceptualizations of both crime and homeland security, therefore, is hopeless, a figment.

Information age networks alter substantially the role of the individual actor—unlike hierarchies; there is an implicit and active role for each member of the network. Responsibility and accountability

shift from the top of the pyramid and are dispersed throughout the corporate body. This is a concept that is hinted at in community policing and made explicit in its neighborhood-driven variant (see Jensen and Levin, 2005).

SEAP translates easily to the world of individual responsibility by increasing transparency. It gives Joe Sixpack some relatively simple indices to the delivery of reliable services.

Once he has been presented concepts in a digestible manner, Joe will have the means of holding his public servants accountable. Criminologists may deride the FBI's crime clock (see Federal Bureau of Investigation, 2002), but it has the virtue of being easily understood by the end consumer. The crime clock created transparency—imperfect, to be sure, but effectively communicating what previously was opaque. The primary weakness of the crime clock for the current purpose is that it records system failures rather than system up-time. System up-time is what we need when it comes to both homeland security and crime.

Isn't the difference between system up-time and system reliability really just a matter of how one looks at it rather than of substance? No. First, reliability is simpler for the user than is failure rate. It is easier to understand how often something works than how often it does not work. Second, system up-time creates hope, opportunity, and an expectation of improvement. Third, measures of system reliability are harder to mold into scare headlines. This last is a non-trivial concern, given the pervasiveness of media and the marketability of deviant frightening events.

Survival in the Information Age: Hardiness and Resilience

As the name implies, the power of terrorism is largely psychological—otherwise, how does one explain our obsession with it beyond other more demonstrable threats to our personal safety (e.g., automotive crashes)? The stress of dealing with a terrorist event, coupled with unremitting media images, can be unsettling for many and overwhelming for some. Consider what will happen in the near future: given the rapid expansion of all types of media, images of violence and carnage will be ubiquitous. If terrorism is not the source of our anxiety, something else will emerge. We literally risk scaring ourselves to death amidst a sea of comparatively unlikely but highly evocative pandemics, terrorist events, cyber Pearl Harbors, car chases, shoot-outs, and the like.

In any environment, there are some who thrive and some who become stress puppies. It is in our interest as a society to encourage the former and help the latter. What is it that differentiates them? There is immense literature on hardiness (a personality construct) and resilience (stability of behavior under assault).

Most recently, two approaches for dealing with the psychological (i.e., most significant) effects of terrorism have emerged. Everly and Castellano (2005) have proposed what they term “psychological counterterrorism,” which they define as “efforts to prevent or counteract the adverse psychological effects of terrorism.” (Ibid: 113).

The goals of psychological counterterrorism are (Ibid.: 41-42):

- 1) to reduce the likelihood that terrorism will be used as a weapon,
- 2) to bolster the psychological resistance of the targets of terrorism (military, emergency responders, civilian),

- 3) to bolster the psychological resilience of the targets of terrorism (military, emergency responders, civilian),
- 4) to facilitate the treatment of those significantly impaired by terrorism
(Ibid.: 41-42.)

Everly and Castellano maintain that, in addition to law enforcement and the military, the public health sector is responsible for ameliorating and thwarting terrorism. They recommend a series of steps to strengthen the courage and resolve of the citizenry.

Levin (2005) takes a more direct, and individual, approach. Like Everly and Castellano, he agrees that the strength of terrorism lies in its ability to frighten and thereby coerce. He summarizes his proposed counterterrorism strategy in four words: “Terrorized? Get over it.” (Levin, 2003:75).

How should we “get over it?” Levin adapts Michael Useem’s business model approach, which he says applies equally to terrorism:

- 1) Focus on what’s working,
- 2) Instill confidence,
- 3) Ensure team camaraderie, and
- 4) Invest in a courageous culture

In short, in World War II, Americans were called upon to sacrifice for the war effort. This included rationing and volunteerism (e.g., victory gardens). The war on terrorism is a different type of war. It requires a different type of sacrifice, more akin to that of the citizens of London during the Nazi V2 attacks. Terrorism will not work unless we allow it to succeed—to prevent that from happening, we would be well advised to follow another of Churchill’s admonitions:

Remember, we shall never stop, never weary, and never give in. (Churchill in Everly and Castellano, 2005: 124).

Taking Control: Neighborhood-Driven Policing

It is axiomatic in psychology that anxiety is reduced when individuals feel they have control over their lives and environment. Indeed, in many ways, the SEAP concept is all about individual rather than government control.

Recently, Levin and Myers proposed a model of policing for the information age which they dubbed “Neighborhood-Driven Policing (NDP).” The premise of NDP is that the police should no longer hold a monopoly on providing safety. Rather, they and the citizenry work as equal partners in promoting homeland and community (Levin and Myers, 2005).

NDP and SEAP are complementary. They share many of the same assumptions and suggest many of the same solutions. *Scenario 3* presents an idealized version of SEAP/NDP. It suggests what could be in the information age.

Conclusion

Homeland security is an evolving process. The information age will no doubt bring much change, at a very rapid rate. To that end, to predict what “will be” is at best a crapshoot and, at worst, a prescription for wasting resources on a future that will never be. In order to deal with a myriad of futures, the authors have proposed a generalized model for homeland security, which combines expected trends with flexibility. This seems to us the best way to traverse an uncertain future.



Scenario 1: Military Policing World

The headline in the Washington Post told the story: “Elite Army Unit Battles Gang in the Streets of Arlington.” Fortunately, thanks to precise planning, crisp intelligence, and the latest non-lethal technologies, no one died. And importantly, what was once considered an intractable scourge in northern Virginia was dealt an apparent deathblow.

The gang itself was impressive: the remnants of MS-13, the R Street Crew, and “professional” freelancers from South America had gotten together in 2008 to form a loose confederation in an attempt to dominate the highly lucrative vice trade and cyber black markets. And, up to this point, they had been highly successful. Thanks to their ability to “purchase” the skills of former operators, engineers, and computer heavies, as well as their understanding of what works in the information age, they didn’t look much like a traditional gang: rather, their somewhat informal, but highly effective structure resembled what many thought an intelligence service should look like in 2015—networked but decentralized and flexible, making and breaking alliances as the need arose. In a nod to Osama bin Laden, whose tactics they emulated, the gang called itself “the Base.”

The Base wasn’t the first or only criminal enterprise to organize itself along these lines. By 2010, the most successful criminal groups employed technologies that had once been the exclusive domain of the CIA. Federal, state, and local law enforcement agencies were flummoxed. Conventional law enforcement tactics had little effect: given the gang’s use of ultra-encryption, conventional wiretapping was useless. As well, their employment of “truth technologies” made infiltration next to impossible. And, given their ruthless nature and sophisticated intelligence networks, few citizens were willing to come forward

and even report crimes to the police. Those who did soon wished they hadn’t.

In spite of the rapidly changing nature of the threat, law enforcement was slow to change its tactics. Truly believing that more resources would handle the problem, policing agencies kept getting bigger rather than smarter. And while traditional problems of information sharing, turf, and hubris had steadily improved since 9/11, the profession wasn’t able to transform itself in time. Three trends converged in the late 2000s, outraging the citizenry. Crime rates began to rise dramatically. If this wasn’t bad enough, police leaders blamed the rise on external factors, such as demographics and economics. Unfortunately for them, citizens and the media remembered the 1990s, when many inside and outside policing had proudly pointed to falling rates of crime, especially violent crime, as proof of law enforcement agencies’ effectiveness. Charges of political cowardice & ineffectual leadership abounded.

In addition, several high profile law enforcement disasters occurred in 2008 and 2009. One involved the high profile kidnapping of a famous actress. At first, the investigation had gone well—the police and the feds, working together, had discovered where the kidnapers had taken her. Unfortunately, a highly risky rescue attempt ended disastrously, with the actress and several law enforcement officers killed. Of course, all of this unfolded under the watchful eye of the ubiquitous media, which broadcast it live for the world to see.

Finally, the threat of terrorism was never far from the public consciousness. While nothing of the magnitude of the 9/11 attacks occurred, many smaller events convinced the citizenry that they were not safe. A radical Islamic group had managed a coordinated attack on two shopping malls in 2007 in which 187 people died. As well, animal rights and environmental groups, whose tactics became

increasingly violent as the decade progressed, succeeded in killing four research scientists and seven corporate executives in separate incidents.

Public confidence in law enforcement all but evaporated. Politicians got the message in the 2008 Congressional elections when several incumbents were defeated by a new generation of ultra neocons who called for an expanded use of the military for domestic matters. While debate about Posse Comitatus raged in Congress, it turned out that the President had already moved on the situation. In the wake of the 2007 attacks, she had authorized a classified directive that the military could do “whatever was necessary” to address terrorism domestically. The Northern Command immediately began commando and intelligence operations within the United States. Utilizing the very latest in technology and psyops, and unconstrained by laws that regulated law enforcement agencies, the military proved effective in reducing terrorist attacks. Buoyed by their success, the Pentagon put forth a two-pronged argument that the military should have an expanded role in police activities.

Both arguments ultimately revolved around homeland security. The first concerned the fact that many terrorist entities utilized criminal activity to fund their activities. Hence, the most effective way to proceed against such groups might be in the criminal arena. Second, they argued that “homeland security” as currently understood was too narrowly defined. Such things as international organized crime, identity theft, economic espionage, drug trafficking and even street gang activity, were direct threats to national security, according to the military. Their arguments proved persuasive. And it didn’t hurt that law enforcement had been largely ineffective in addressing these areas. One military commander put it this way: “Give us the authority and we’ll give you a REAL war on drugs!” Senior law enforcement officials privately anguished

that they had ever used the phrase “war on...” to describe anything.

As the deployment of the military gradually expanded within the United States, civil libertarian groups and law enforcement agencies became unlikely allies. In one memorable event, the head of the ACLU and the Director of the FBI issued a joint press release decrying the decline of civil liberties in America.

But it did little good. In fact, the train had already left the station. The public was willing, even eager, to surrender civil and privacy rights if it led to enhanced safety, or at least the perception of enhanced safety. With every domestic military success, the public cheered and demanded that the Defense Department be given greater responsibility for traditional criminal matters. By now, military checkpoints and random vehicle stops were commonplace. Title III authority, which had governed law enforcement’s use of wiretaps, was considered a quaint anachronism. By 2012, the NSA was listening in on more domestic phone calls than international ones. The lack of legal barriers regarding the use of the military was especially seductive—why bother with “pesky” legal restrictions if you didn’t have to?

The military had even been successful in arguing that some especially notorious criminals were “enemy combatants.” To that end, they began sharing residence in Gitmo with al Qaeda remnants who had been there since the early part of the century.

As the military’s influence in domestic criminal matters increased, law enforcement’s responsibilities, and resources, declined. By 2015, most police agencies found themselves enforcing traffic laws and handling misdemeanor and minor felony offenses. As the century progressed, the gap between law enforcement’s capabilities and those of its adversaries continued to widen. Fewer

people wanted to go into policing; those that did generally did not possess the routinely outstanding qualities found in those who chose military careers. Progressive programs like evidence-based policing and restorative justice were but a memory. With their aging fleet of vehicles, substandard computer systems, and lack of qualified personnel, most police agencies could barely keep up with even answering basic 9-1-1 calls.

While some in the public waxed nostalgic about the good old days of the “cop on the beat,” most barely noticed. Perhaps most telling, the highest rated on-demand 3-D television show was titled “SEAL Patrol.” Its premise: televising a real SEAL team on patrol...in Los Angeles.

Scenario 2: Private Policing World

It began in 1997 as a company that sold credit data to the insurance industry. But over the next seven years, as it acquired dozens of other companies, Alpharetta, GA-based Choice Point Inc. became an all-purpose commercial source of personal information about Americans, with billions of details about their homes, cars, relatives, criminal records and other aspects of their lives. As its dossier grew, so did the number of Choice Point’s government and corporate clients, jumping from 1,000 to more than 50,000 today. Company stock once worth about \$500 million ballooned to \$4.1 billion.¹

February 22, 2015: Special Agent Christine Allen initiated the tele-conference from her squad’s secure commo-room. Her case review was in two days, and if she didn’t have her act together, her supervisor would have her for breakfast. Some years ago, the FBI had adopted a modified version of the old New York COMPSTAT model to demonstrate its seriousness concerning accountability.

Christine needed to gain a full update on the cases she was supervising: her interactive Blackberry XII helped her out here, organizing and managing the information and intelligence she needed to demonstrate to her superiors that she was managing her resources appropriately.

The first one to sign in was Elliot from Universal Business Affiliates (UBA). Christine’s squad handled mostly fraud cases—in the old days, there was a bifurcation between “fraud” and “cyber” investigations. Today, that distinction was meaningless, as almost every crime involved the use of a computer. Indeed, the notion of a separate “cyber” category was a curious artifact of a time when computers were little understood by the policing community

Elliot reported that the recent upgrade to UBA's tracking software had proven effective in tracking the latest cyber-scam to an ISP in Sumatra. Of course, the scammers had sensed the oncoming approach of the authorities and had remained one step ahead. But the good guys were catching up. Among other things, cyber signatures and other identifying data had been obtained. As soon as Jolene from MegaInfo signed on, Christine asked her for a full work-up on the data. Almost instantaneously, Jolene came back with suspected names, identifying data, and likely next moves of the group.

Once supplied, Christine relayed the information to the "Quantam Commandos," a 24/7 FBI response group that would set up a digital and, as necessary, physical surveillance to nab the perps.

Christine, Elliot, and Jolene were all part of the FBI's Sacramento Fraud Task Force. Each had sworn powers. And while Christine was an FBI agent, Elliot and Jolene were DOJ contractors.

The Sacramento Task Force might have seemed odd to a law enforcement officer of the late 20th century. At that time, task force members were generally all sworn members of policing agencies. By the early days of the 21st century, however, it had become abundantly clear that the information age had rendered obsolete any notion that policing, in and of itself, could remain effective against an elusive, dynamic, and techno-savvy adversary.

A large part of the problem was fiscal; the notion that an agency had to decide two or three years out what its major challenges would be was ludicrous in an age of exponential change and growth. Instead, Congress had been forced to conclude that only by allocating large sums for discretionary spending and allowing the purchase of off-the-shelf technologies and services could any law enforcement organization hope to retain relevance.

Cracks in the public policing foundation had begun to emerge in the late 1990s, when progressive local agencies began to outsource various functions, such as the guarding of crime scenes and the transporting of prisoners, to private agencies that were able to perform these functions at a much reduced cost.

At the same time, in the interest of economics, some agencies began to consolidate; others regionalized particular functions, such as jails, communications systems, and evidence collection facilities. While this saved money, it conspired to undermine local citizen control.

Affluent communities struck back: gated developments and private security forces proliferated in record numbers. The typical private security force of 2015 resembled a police department much more than it did a collection of security guards. Indeed, most members were sworn and performed both patrol and investigative functions. This resulted in no small degree from various Criminological studies dating from the 1970s that showed that the duties performed by those officers who initially responded to a situation were the ones most likely to solve the case. As a result, private security firms successfully argued that, since they generally beat the police to crime scenes, they should initiate logical investigative tasks. These included securing the scene, interviewing witnesses, and conducting neighborhood canvasses. Many public-policing agencies soon realized that they couldn't beat the private sector: like their federal brethren, they decided to work with them instead. Perhaps the biggest problem the public sector had was private poaching. In the late 1990s, small agencies bemoaned the fact that many of their most talented folks were recruited by the better-paying feds and larger agencies. By 2015, poaching had shifted to the private sector, which could afford better

salaries, benefits, and equipment.

If the news was good for the rich, it wasn't so good for the poor. Since the wealthy had "gotten theirs," they were less inclined to fund public policing agencies. To that end, the lean budgetary years of the early 21st century were recalled fondly by police administrators as a time of downright largess. By 2015, even 9-1-1 response in some large cities was threatened. Publicly, police chiefs expressed concern over the burgeoning Citizen Vigilante Movement that was gaining momentum in many of the country's worst neighborhoods. Privately, most conceded that citizens needed to do something to protect themselves if the police couldn't.

In sum, the private policing movement of 2015 was a mixed bag: for those agencies and communities that could afford it, the private sector provided resources and expertise that could not be easily duplicated in the public sector. Not everyone was comfortable with placing so much power in the hands of the private sector, however. Indeed, privacy advocates found themselves in a strange position, championing those very agencies they had steadfastly criticized over the years. As well, what had once been a profession that had as its goal "equal protection under the law" was characterized by wildly differing standards, objectives, and results.

Back on the Sacramento Task Force, success was at hand. Thanks to UBA's state-of-the-art tracking software, the scammers were located in a small suburb outside Philadelphia. The cyber-SWAT team had successfully apprehended them and was able to gather a treasure trove of evidence.

As so often happened, one of the members of the Task Force represented a private company that had been a victim of the scam. As Christine prepared her case for submission to the U. S. Attorney's Office, the private company rep quietly

conferred with his superiors about how to best preserve the interests of the company. Sometimes these conflicts proved acrimonious; occasionally, they were insurmountable. Christine, however, was hopeful. And regardless, a couple more bad guys were off the street. There were only several thousand more to go.

Endnote:

1Robert O'Harrow Jr. "Choice Point Quietly Finds Wealth in Information: In Age of Security, Firm Mines Wealth Of Personal Data" *The Washington Post*, January 20, 2005.

Scenario 3: Neighborhood-Driven Policing World (NDP) in the context of Systems Evolution and Applications Protection (SEAP):

By early in 2012 it had become apparent even to the media that the system of governance in the U.S. was failing terribly. Representative democracy had become so hierarchical that even its staunchest defenders believed that its expense and its ineffectiveness at the local level had become as bad as the “problems” it was trying to fix. Worse, government programs had nearly destroyed the sense of community in most lower and middle class communities. A radical plan was hatched—decentralization of both resources and forces.

What did the plan call for? Taking its key from “government of the people, by the people, and for the people”, the plan was marketed as people taking control of their own fate. While there had been initial worries of vigilantism, it turned out that when reasonable people were given a choice, they chose peaceful resolution of conflict. This outcome was not unlike the social process seen in what is misunderstood as the “wild” west of the U.S. in the 19th century. For example, Tierney (2005) wrote, ““Pure bilge,” Dr. Parker told me. “There wasn’t an awful lot of violence in Deadwood except for the crooks and drunks killing each other. When everybody has a gun on his hip, they tend to avoid confrontation.” Unwittingly following the Deadwood model, many communities in the U.S. of 2012 quickly adapted to their new-found empowerment.

Fortunately, Jensen and Levin (2005) had edited a volume providing a variety of choices that might enable communities to adapt to the new world they are facing in the 2015 of today. Smallsville residents, knowing that they must chose their style of governance anew, had studied Jensen and Levin but also had articulated their own values—which

turned out to be consistent with SEAP. What they wanted was stability, responsiveness, and ability to adapt to changing needs and contexts. They chose an NDP/SEAP model and have been running with it for several years at this point.

The citizens still gripe a bit because they are expected to spend more time with their neighbors and less time with their VideoScreen Lenses® and Ubiquitous Communicators® and other optical/electronic distracters. Particularly the younger (teenangel) males whined until the older generations asserted themselves, teaching the importance of duty to others. That latter value, seemingly moribund for decades, turned out to be pivotal in the survival of the community, as we shall see shortly.

As the governmental hierarchy weakened, opportunistic threats became manifest. Terrorists, gangsters, traditional organized criminals, and even geopolitical invaders became significant threats to the peace and tranquility of the lives of citizens in many localities. As the hierarchy’s vulnerabilities increased, we saw demonstrated again that nature abhors a vacuum. Perps of all descriptions stepped into the organizational flaws and cracks. Citizen safety plummeted in most places, while anxiety levels climbed and productivity dropped like a rock.

Smallsville, however, was an odd exception. Smallsville was an island of tranquility in a sea of chaos. No gangs, no terrorists, and no street criminals stayed for very long. Why?

To the social anthropologists who have been studying Smallsville for a few years now, the answer became obvious. Smallsville’s outcome was very different because its choices had been very different from those taken by most localities. Instead of putting lipstick on the hierarchical pig, Smallsville had taken a comprehensive approach to solidifying its social structure, and even a casual walk down Main Street made the results obvious.

People in Smallsville actually talk to one another, instead of merely passing one another on the sidewalk. More important, residents embrace the Deadwood/Peel ethos—each takes an active role in the protection of the community. For some, this takes the Deadwood model literally: citizens armed with the latest in lethal and non-lethal weaponry provide support for Heinlein’s contention that “an armed society is a polite society” (Heinlein, 1997). Still others of a less physical bent use their communicators to maintain real-time audio and visual communication with the police. And citizen involvement in such arenas as restorative justice, mediation, and mentoring has never been higher. If nothing else, the Smallsville experiment contradicts the industrial age notion that a single model of policing is desirable. Indeed, like everything else in the information age, each citizen’s unique talents and views of the world are important in contributing to the safety of the community. While “law and order” may have once been considered a conservative value, “community safety” is universal, cutting across the entire political spectrum

The most significant aspect of Smallsville’s version of homeland security is its adoption of a systems approach to neighborhood-driven policing. Because law enforcement now had few calls for violence of any sort and because citizens embraced enhanced responsibility for themselves and their neighbors, police were free to evolve—and have evolved—into social and security advisors.

The advice of police is now actively sought when every building permit is issued, when every landscaping plan is approved, and when changes in social institutions (schools, hospitals, etc.) are discussed. The police have become active and valued professional partners rather than blue (or no) collar, combat-capable, garbage collectors.

As a result, Smallsville now has fewer

police (although it pays much higher salaries than previously), and far higher levels of safety and security. Business and industry is thriving in Smallsville, and innovation incubators abound. Neighboring communities and even towns in foreign countries find themselves drawn to Smallsville, hoping to adopt the Smallsville approach to homeland security, and to life.

Endnotes

- i. The authors may be contacted at levinb@brcc.edu.
- ii. Dr. Levin is a Professor at Blue Ridge Community College, a Reserve Major in the Waynesboro, VA Police Department, and the Vice Chairman of the Futures Working Group.
- iii. Dr. Jensen is a Supervisory Special Agent in the FBI’s Behavioral Science Unit and the Chairman of the Futures Working Group.
- iv. *Jacobellis v. Ohio*, 378 U.S. 184, 197 (1964)
- v. Department of Homeland Security (2004) at URL <http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0413.xml> accessed 03/09/2005
- vi. We base our conclusion on a rephrasing of Parkinson’s famous law: “Work expands so as to fill the time available for its completion” [Parkinson, Cyril (1958). *Parkinson’s Law: The Pursuit of Progress*. London: John Murray.] In a bureaucracy, the size of an agency’s turf and its level of resources generally expand to the extent it successfully defines its mission in line with the cause du jour.
- vii. In futures research, it is considered limiting to talk about the future. Instead, most futurists discuss possible alternative futures, oft-times by utilizing scenarios, as we have chosen to do here (see Schwartz (1999) for an in-depth explication of scenario construction and use.)
- viii. Homeland security grants will be the early 21st century’s equivalent of the COPS grants of the 1990s.
- ix. See, for example, “PERF Asks FBI to Focus on Terrorism.” (March 9, 2005) *Police Magazine* at URL <<http://www.policeone.com/policeone/frontend/parser.cfm?object=Columnists&tmpl=article&id=77187>> accessed 03/09/2005.
- x. Many of these were taken from the National Intelligence Council’s *Mapping the Global Future* (2004) at <http://www.cia.gov/nic/NIC_globaltrend2020.html> accessed 03/09/2005.
- xi. In his analysis of al Qaeda members, Sageman (2004) notes that most did not fit the stereotype of the young, disaffected, terrorist. Most were well-educated, married, and had been raised in a secular household. The common thread that Sageman noted was that most had drifted into radical Islam after they had left their native countries in search of better-paying jobs. Many had ended up in Europe and had drifted into radical mosques after feeling lonely and isolated in the non-Muslim society.
- xii. In this and the following sections, we are interested only in those groups engaged in criminal behavior. The First Amendment of the U.S.

Constitution guarantees protection for those individuals who participated in free speech and legitimate protest activities.xiii. Smart (2005) differentiates “developmental” change from “evolutionary” change as follows: evolutionary relates to sudden, abrupt, difficult to predict change while “developmental” refers to the steady, predictable changes that one can foresee (e.g., the increasing importance of the Internet is developmental; an asteroid striking the earth is evolutionary). Readers should employ both in considering possible futures; the authors have found that a scenario-based approach is generally the preferred method for accomplishing this.

xiv. Virtual groups providing the same rewards and emulating the same dynamics that physical groups historically have.

xv. For example, successful, unbiased elections may force heretofore terrorist groups to attempt to become more involved in the political process.

xvi. “... team of international experts concluded that the world is at risk on a variety of fronts, including a skyrocketing runoff of nutrient-rich farm waste that’s killing swaths of the world’s oceans, a massive wave of animal and plant extinctions and a planet that’s growing warmer.” (Borenstein, 2005)

xvii. See Kessler (2004) for the story of William Krar, an alleged white supremacist, who was discovered in possession of fully automatic machine guns, remote-controlled explosive devices disguised as briefcases, 60 pipe bombs, nearly 500,000 rounds of ammunition and enough pure sodium cyanide “to kill everyone inside a 30,000 square foot building, according to federal authorities.” (Ibid., pg.1)

xviii. Ned Ludd was a legendary (perhaps apochryphal) figure in 19th century England who destroyed two power looms, thus inspiring weavers (who were displaced by the looms) to form a guerilla army of sorts. A “Luddite” is one who eschews technology <“What is a Luddite?” (undated)>.

xix. Sir Robert Peel authored his famous nine principles for policing in 1829. One of these held that “Police, at all times, should maintain a relationship with the public that gives reality to the historic tradition that the police are the public and the public are the police; the police being only members of the public who are paid to give full-time attention to duties which are incumbent on every citizen in the interests of community welfare and existence (Peel, 1829).”

References

- Borenstein, Seth (2005) “Scientists warn of Earth’s declining environmental health,”. *Knight Ridder* at < <http://www.realcities.com/mld/krwashington/11260255.htm> > accessed 4/1/2005.
- Clarke, Richard A. (2005) “Ten Years Later,” *Atlantic Online* at < <http://www.theatlantic.com/doc/prem/200501/clarke>> accessed 03/12/2005.
- Everly, Jr., George S. and Cherie Castellano. (2005) “Psychological Counterterrorism and World War IV,” *Ellicott City, MD: Chevron Publishing.*
- Federal Bureau of Investigation. (2002) “Crime Clock,” *Crime in the United States*. Washington, D.C.: Federal Bureau of Investigation at < http://www.fbi.gov/ucr/cius_02/html/web/offreported/crimeclock.html > accessed 04/25/2005.
- Friedman, Thomas L. (2000) “The Lexus and the Olive Tree,” New York: Anchor Books.
- Gurr, T. R. (1970). “Why Men Rebel,” Princeton NJ: Princeton University Press.
- Heinlein, R. A. (1997). “Beyond This Horizon,” The New American Library.
- Jensen III, Carl J.& Bernard H. Levin, eds. (2005). “Neighborhood-Driven Policing,” Washington, D.C.: Federal Bureau of Investigation at < http://www.fbi.gov/hq/td/fwg/neighborhood/neighborhood_driven_policing.pdf > accessed 04/25/2005.
- Kessler, Jim (2004). “Outside View: Who is William Krar?” United Press International at < http://www.upi.com/view.cfm?StoryID=20040311_030156_8181r > accessed 04/22/2005.
- Kurzweil, Ray (1999). “The age of spiritual machines: When computers exceed human intelligence,” New York: Viking.
- Levin, Bernard H. (2003). “Risk and terror: Responses to perceived threat,” *Police Research & Management* 6(1), 69-76.
- Levin, B. H. and Myers, R. W. (2005). “A Proposal for an Enlarged Range of Policing: Neighborhood-Driven Policing,” (NDP). In Jensen and Levin (op. cit.)
- National Intelligence Council (2004) “Mapping the Global Future,” at < http://www.cia.gov/nic/NIC_globaltrend2020.html >accessed 03/09/2005.
- Peel, Robert (1829) “Sir Robert Peel’s Nine Principles,” *New Westminster Police Service* website at < <http://www.nwpolice.org/peel.html> > accessed 06/26/2005.

Sageman, Marc (2004) "Understanding Terror Networks,"
Philadelphia: University of Pennsylvania Press.

Schwartz, Peter (1999). quoted in *Work in the Knowledge
Driven Economy*. "Future Unit: Department of Trade
& Industry, United Kingdom," at < [http://www.park.
cz/soubory/workinde.pdf](http://www.park.cz/soubory/workinde.pdf) > accessed 9/30/2003.

Shuster, Henry (2005) *An unholy alliance: Aryan Nation
leader reaches out to al Qaeda*. CNN.com at URL
< [http://www.cnn.com/2005/US/03/29/schuster.
column/](http://www.cnn.com/2005/US/03/29/schuster.
column/) > accessed 4/1/2005.

Smart, John. (2005). *Homeland Security: 2015*. Presentation
before the Futures Working Group, 03/011/2005,
Phoenix, Arizona.

Tierney, J. (2005). "The mild, mild west," New York Times,
25 June. < [http://nytimes.com/2005/06/25/opinion/
25tierney.html?>pagewanted'all](http://nytimes.com/2005/06/25/opinion/
25tierney.html?>pagewanted'all)

U.S. Department of State (2004). "Patterns of Global
Terrorism," 2003. < At URL [http://www.state.gov/s/
ct/rls/pgtrpt/2003/31711.htm](http://www.state.gov/s/
ct/rls/pgtrpt/2003/31711.htm) > accessed 3/12/2005

"What is a Luddite?" (Undated) at URL < [http://www.usu.edu/
sanderson/multinet/lud1.html](http://www.usu.edu/
sanderson/multinet/lud1.html) > accessed 3/13/2005.

World of Quotes (undated). *Quotes of Winston Churchill*
at URL < [http://www.worldofquotes.com/author/
WinstonChurchill/1/](http://www.worldofquotes.com/author/
WinstonChurchill/1/)> accessed 4/22/2005.

Law Enforcement Technology 2015

**Charles “Sid” Heal, Thomas Cowper
Andreas Olligschlaeger**

Introduction

On January 28, 2001, the Tampa Police Department used a little-known technology called biometric facial recognition to scan the faces of 71,921 fans attending Super Bowl XXXV for known criminals and terrorists.

On November 14, 2002, the New York Times published an article by William Safire entitled “You Are a Suspect,” accusing the Department of Defense of creating “computer dossiers on 300 million Americans,” an “Orwellian scenario” leading to a police state that would be created by an advanced data mining project called Total Information Awareness.

On Wednesday, October 21, 2004, a young woman in a crowd of some 60,000-80,000 baseball fans celebrating the historic victory of the Red Sox over the Yankees was killed by a pepper-dispensing projectile fired from the less-lethal weapon of a Boston police officer.

On Thursday, February 4, 2005, after spending \$170 million, lawmakers in Congress criticized the FBI for continuing problems associated with its Virtual Case File system to manage criminal and terrorist investigations, and their inability to determine when or if the system would become fully operational.

Technology and law enforcement have always been a complicated and controversial mixture

of crime fighting strategies, labor-management relations, agency budget battles, social policy, Constitutional law and politics. From the adoption of fingerprint identification and the establishment of forensic crime laboratories in the early 20th Century to the use of 2-way radios, radar and laser guns and Plymouth Roadrunners in its latter half, the use of technology by police has been fraught with problems that span the breadth and depth of the law enforcement realm. While there have been many successful implementations throughout the last century, more often than not new technology initiatives, big and small, have fallen far short of expectations, both of the police who use them and the public upon which they are used.

21st Century technology is going to further exacerbate this enduring trend over the next ten years. There are more technology options for law enforcement today than at any time in history and these technologies and their associated systems are more sophisticated, intricate and powerful than ever before. Every new technological breakthrough with application to law enforcement, or of use by criminals and terrorists, brings with it new and unique difficulties and dilemmas for the police and their communities. Every new system or network intended to improve policing can also bring with it unwelcome financial hardship, organizational transformation and public scrutiny to agencies that may not be prepared for them.

Technology is a multi-edged sword that will cut in many directions. Its use for law enforcement and homeland security in the coming years is essential if we are to provide for the safety of our cities and neighborhoods, but used unwisely by government it could have an adverse impact on civil liberties and social stability. Technology will be used by criminals and terrorists, giving them more opportunities for crime, more tools to use against the innocent, and a greater ability to avoid apprehension.

And as it permeates more of our world and we become more dependent upon its networks and systems, technology makes us more vulnerable to the severe social and economic disruptions that can be caused by individual criminal and terrorist acts, making the job of stopping those acts an essential component of maintaining both security and liberty.

To accomplish this goal—providing both security and liberty—as we continue the march toward 2015 will not be easy. Dealing with ongoing and longstanding police challenges, adopting new technologies, modifying operational processes to cope with new threats and adapting to a rapidly changing world will severely tax the capabilities of law enforcement agencies and law enforcement officers alike. This article examines a few of the benefits, capabilities, problems and implications of just some of the technologies, systems and networks that will confront and confound the law enforcement profession over the next decade.

Coming Out of the Dark Ages

Like many government agencies, law enforcement has traditionally been slow to adopt new technologies. This is especially the case for information technology. By the early 1990s most law enforcement agencies were still at the level of late 1970s/early 1980s technology. The COPS MORE program in the early to mid 1990s is one example of several programs that provided a much-needed catalyst to law enforcement. It gave those agencies that chose to do so an opportunity to invest in advanced information technology. At the same time the National Institute of Justice was providing grant funding for research into ways in which computer technology could be used to go beyond simple data entry and retrieval. The Drug Market Analysis Program (DMAP), for example, sparked an interest in crime mapping and was one of the main factors

leading to the establishment of the NIJ's Crime Mapping Research Center, recently renamed MAPS, as well as the now almost universal adoption of crime mapping.

By early 2000, law enforcement was beginning to emerge from the Dark Ages but the events of 9/11 only served to emphasize the fact that law enforcement information technology was still inadequate to the task. For the most part, police agencies across the country were in possession of the bits and pieces of information that in hindsight might have prevented the attacks, but the policies, procedures and technologies were not in place that would have allowed analysts to see the big picture. Today, five years after 9/11, law enforcement is not much further ahead in its ability to “connect the dots” than it was in 2000. Many efforts are underway to standardize law enforcement information (Embley, 2002), provide the infrastructure for widespread sharing of information, enact legislation to permit information sharing, and warehouse data and deploy technologies such as data mining, link analysis and other analytical techniques. Nevertheless, we are realistically still a number of years away from seeing them implemented and coordinated on a national scale.

It is critical that as we proceed into the next decade law enforcement have timely access to modern information technology. Our recent history waging the war on terror has clearly shown that the failure to do so can have serious consequences. Over the next ten years, digital chips and wireless networks will turn more and more previously standalone technologies into information technology nodes, exponentially increasing the amount of information with significance to law enforcement. By 2015 virtually all technology will be information technology. Yet in spite of these emerging changes and our recent efforts to improve, we continue to see well-publicized and well-documented information

technology failures such as Total Information Awareness (TIA), the FBI's Trilogy and Virtual Case File projects, the large-scale abandonment of the MATRIX program and numerous others. The opportunity to avoid similar failures in the future and bring law enforcement out of technology's dark ages is largely dependent upon how we deal with the following issues.

The Government Technology Lifecycle

The first thing police officers and police managers need to understand is that technology in general—and information technology in particular—is evolving at an accelerating rate of change. What this means is that the interval between significant technology innovations is decreasing over time. Private industry, the military and even consumers have been adapting to this accelerated change by replacing or upgrading more often than they did even five years ago. For private industry, this is necessary to avoid falling behind the competition; for the military, it is imperative for victory on the battlefield. Civilian government, on the other hand, has not discovered a mechanism to adequately streamline its processes and overcome the centralized bureaucratic hurdles to timely technology procurements. While private industry has been replacing or upgrading technology every 2-4 years, and the military pursues an ongoing multibillion dollar “transformation” program, the procurement lifecycle in civilian government remains extremely slow. Accelerating change will create an even wider technology gap for civilian law enforcement unless something is done to shorten the government technology lifecycle.

Funding

While the technology lifecycle for

government remains inadequate for a changing world, many, if not most law enforcement agencies still lack the funding to keep up with technology. Few agencies have enough money in their budget to allow for continuous upgrades and maintenance of computer systems. Typically they are dependent on grant funding to upgrade computer systems. Indeed, in the past it has been federal funding, such as COPS MORE, or state block grants that has been the primary catalyst for technology adoption at the state and local level. When funding becomes available agencies upgrade, but the array of need usually outstrips the available money. Federal funding is often diverted away from information technology projects to procure other (and also much needed) items such as less lethal weapons, bulletproof vests, vehicles and radios. The problem with this is that agencies pit one technology procurement against another, they remain stagnant or fall behind in their ability to process an ever increasing amount of information, and in the long run keeping up with technology becomes more expensive, disjointed and inefficient. For example, if a police department has to wait five years until they can upgrade to a new version of a particular piece of software they will often find that in order to be able to upgrade they will also have to purchase new hardware. In turn this might result in the need for a complete overhaul of a department's computer systems, which is not only an expensive proposition but might make it impossible for the department to upgrade because funding is only available for the software.

Leadership

Technology today is an integral part of any successful police agency and as such the impact of leadership upon technology procurement, policies and programs is critical. As we approach 2015, the overall law enforcement effort will be hampered by police leaders who do not understand technology and accelerating change, who do not appreciate

the advantages that well managed information technology systems can bring their agency, and who continue to focus resources on Industrial Age methodologies based upon traditional cultural attitudes toward information and information-sharing. There are many examples today of large, medium and small police departments that stand out from the norm and do have access to state of the art information systems. In almost all cases the main reason those departments have been successful is strong leadership, either within the department via the Chief of Police or other high ranking official, or externally via a city administrator or IT department head. By contrast, many police chiefs view information technology as less important than other pressing issues. They do not value the contribution information technology can make because they are simply not aware of what modern information systems can do when implemented correctly.

Marketing New Technology

It is fair to say that most governments have never been very adept at marketing new ideas. This is especially true for law enforcement. A good example of this was the Total Information Awareness (TIA) project, an information technology research and development program designed to improve law enforcement's capacity to handle the rapidly increasing amount of information in our world and make rational decisions based upon it. The goal of TIA was to develop information technology that is desperately needed by law enforcement in order to prevent future terrorist attacks. Yet there was little public dialogue about what the project was hoping to achieve, nor were there sufficient guarantees that the project would not unduly violate the public's right to privacy. In the end the project died from lack of a true understanding of the technology, its capabilities and

its purposes, as well as the public's concern about Big Brother.

The same fate awaits the next generation of information technology for law enforcement unless police leaders can effectively educate policy makers, the media and the public as to why IT is critically important to preserving, and not infringing upon, civil liberties.

Disconnect between IT and Law Enforcement Practitioners

One issue that has historically hampered the development of law enforcement information technology is the fact that information technology and law enforcement practitioners tend to have difficulties communicating ideas to each other. Because neither side understands the other's work, many efforts to implement information systems have failed. For example, law enforcement administrators often severely restrict the functionality of information systems by needlessly limiting access to information. Conversely IT practitioners have been known to limit system functionality by needlessly locking down certain functions for ease of maintenance.

Mega Projects vs. Living Systems

While private industry certainly has had its share of failures, government agencies seem to have more problems succeeding with the implementation of large technology projects. Due to the details and complexities associated with large technology projects it is easy for law enforcement agencies to lose focus and become overwhelmed, primarily because they lack in-house expertise to guide the project. More often than not, the result has been millions of wasted taxpayer dollars and little or no advancement in the police use of information technology. The problem is that ideally, a law enforcement information system should never be

“finished.” Rather, it should be an ongoing project, a “living system” that evolves over time. Creating a new mega project from scratch every 5-10 years is not only counterproductive, but also inefficient in terms of cost and increased agency turmoil. In the long run it is much cheaper and operationally more effective to create a living system that continuously scales and expands through the upgrade of components and software as new technology becomes available.

New Technologies: On the drawing board today, on the street tomorrow

Law enforcement will continue to face many technology related challenges over the next ten years, not only with respect to obtaining and maintaining new technologies, but also in terms of implementing policies and procedures that will allow the free exchange and processing of information without unduly violating the public’s constitutional rights and privacy. While there is no guarantee that information technology will, for example, prevent another terrorist attack, the failure to implement it will almost certainly result in another missed opportunity to prevent attacks on U.S. soil, should such an attempt be made. It is therefore inevitable that we will see an increasing use of other advanced technologies, by state and local law enforcement many of which are currently only available or affordable to federal agencies, the military and large corporations.

UAVs. Unmanned aerial vehicles (UAVs) will undoubtedly begin to augment conventional police helicopters as law enforcement eyes in the sky, especially at crime scenes. UAVs being tested for police use today are light weight and can be set up, deployed and controlled by one or two officers in a relatively short time. By 2015 ultra-light UAVs of many different types and will be able to deploy

directly from patrol cars and function autonomously, providing digital information for surveillance, pursuits, traffic enforcement, tactical operations and any other law enforcement mission that benefits from aerial observation.

Running on a combination of battery and solar power, these UAVs will be equipped with small electric motors, wireless cameras, sensors, devices, and GPS locators. They will be capable of loitering in one location at a preset altitude for hours or following a programmed route while sending real-time data to both officers on the ground and incident commanders. And unlike helicopters, these UAVs will be nearly invisible while in the air, have almost no noticeable noise signature from the ground and will be very inexpensive to purchase and operate, making them widely available for law enforcement operations.

Robotics. Robots will also begin to proliferate over the next ten years. Dozens of different models of robots are available today suitable for a variety of purposes and in the near future the numbers and types of robots available for law enforcement will multiply. Market estimates predict that within a few years millions of robots will be operating in our world. Under development today are small snake-like robots for operation in pipes and confined spaces and robots that climb walls using technology that mimics the biological capability of the gecko lizard. Police robots have been confined to the larger wheeled and tracked types that are equipped with cameras, robotic arms and shotguns but in the future these platforms will be used for many different missions such as area and perimeter security, surveillance, search and rescue and hauling equipment.

But perhaps the biggest innovation to hit the UAV and robot market will be their increasing autonomy and ability to coordinate with each other to perform tasks as a group or “swarm”. A

major technology initiative of the U.S. military, the autonomous operation of UAVs and robots will be commonplace by 2015 adding to their usefulness and freeing up police officers otherwise tasked with their operation or close supervision. For example, a police officer on patrol might have an assigned UAV and robot equipped with video cameras, microphones and sensors that could perform many different tasks to enhance that officer's performance. They might be affixed to the patrol car when not needed or continuously roam the area around the officer providing important information that would increase the officer's situational awareness. In a pursuit situation the UAV might launch and track the fleeing vehicle or person allowing the officer to follow from a distance at a safer speed. The robot might simultaneously perform other tasks to aid the pursuit such as helping to alert traffic at approaching intersections or following the suspect into areas where the UAV cannot follow, such as tunnels or buildings. The officer, robot and UAV would form a coordinated team working together to accomplish their assigned mission, adjusting and adapting as the situation demands.

Biometrics. One of the biggest problems confronting law enforcement today is the ability to positively determine a person's identity, especially in relation to the on-going wars on crime and terrorism. In 2015, biometrics will have advanced to the point that personal identification will be highly accurate and near instantaneous. Biometric identification systems use a person's unique physiological or behavioral characteristics to determine their identity, matching for instance, a real-time scan of a person's features with a digital record of those features previously scanned and stored in a database. Commonly scanned characteristics are fingerprints, retinas, facial features, speech patterns and hand geometry but there are numerous other unique identifiers that may be used.

Being adopted today in many commercial settings some retailers in high-security environments, including the banking industry, and biometrics systems of 2015 will be multimodal, using several different biometrics at the same time to increase accuracy. The days of signing checks and credit card receipts or remembering Personal Identification Numbers (PIN) will have long passed and it is likely that within ten years the courts and other government agencies could begin requiring biometric identification in place of signatures on driver's licenses, bail bonds, passports and the like. While the courts will certainly limit the extent to which they can be used, by 2015 the technologies may be ubiquitous in the private sector, thus mitigating the privacy controversies we experience today. Indeed, the growing problems of identity theft and fraud coupled with their ease of use and the protections afforded by biometric identification could mandate its widespread use.

Electronic Monitoring. Perhaps equally important to the identification of individuals is the ability to monitor and track their movement when necessary. By 2015 this will be easily accomplished using various attachable and implantable devices placed on suspects, convicted criminals and other objects of interest such as personal property and evidence. Many of these technologies are already on the market such as "EZ-Pass" transponders for toll-road access, cell phones for E-911 location and On-Star devices in new cars. Others are under development. The Radio Frequency Identification (RFID) chips and GPS receivers that make this location and tracking possible will proliferate in the coming years as they become smaller and cheaper to manufacture. There are currently implantable RFID chips for humans, and several companies are working on implantable GPS receivers that will eliminate the need for an externally worn device. By 2015 these technologies will be commonplace within

our environment and will work together to enable tracking of anyone and anything.

For example, this technology will allow for secure “home detention” of suspects or non-violent convicted criminals. A suspect may be permanently assigned to a home, restricted to certain neighborhoods or communities, or allowed to travel to and from work along specific routes and at specific times of day. If a suspect diverts beyond the prescribed parameters the system could automatically alert local police and transmit his present location. Further, parameter alarms will prohibit suspects on probation or parole from violating terms of their release, such as being within a given distance from a spouse, school or another parolee. This system should prove to be far more cost effective than total incarceration and could be used for a wide variety of “low risk” crimes such as drunk driving, shoplifting, and so forth. It could also be used for some types of crimes, such as spousal abuse, minor assaults, and similar offenses but with more restrictive circumscriptions. Depending on the court sentence and circumscriptions, such a system allows a suspect to continue earning a living and greatly reduces the burden on the community for the necessary supervision.

Data Mining. All of these digitally based technologies and many others that will emerge generate a tremendous amount of data that will need to be managed, a process that will continue to be one of law enforcement’s biggest challenges in the Information Age. Consider the massive amounts of data that are expected to be collected as a result of information sharing. Because the data are compiled from various sources it will be difficult to match similar records. Last names can be spelled differently, pieces of information might be missing, and there are rarely unique identifiers such as social security numbers that will guarantee an exact match. Such issues are important not only because we want

to avoid missing potential matches, but also because we wish to avoid taking erroneous actions based on false positives.

To accomplish this within today’s homeland security environment, made up of extremely large data sets, it is inevitable that law enforcement will eventually use today’s most controversial information technology—data mining. Manually sifting through large amounts of information for a few small bits of information critically important to solving a problem is humanly impossible unless an analyst knows exactly what he or she is looking for and where to find it. This is why practically every area of human endeavor, from global banking to disease control, is developing and using data mining technology. In this respect, data mining can be of tremendous help to law enforcement in stopping crimes and attacks before they occur or assisting criminal investigators in their aftermath.

There are essentially two types of data mining: looking for known patterns or detecting previously unknown patterns. The former is the most commonly implemented type of data mining and is well researched, with an extensive available literature (here omitted). Detecting previously unknown patterns however is far more complex and requires more sophisticated algorithms: this latter area is the realm of DARPA’s ill-fated Total Information Awareness project. Data mining research efforts will continue to be concentrated in this area because it potentially produces the most promising results. Like health officials striving to identify the outbreak of serious diseases before they become epidemics, or bankers trying to stop identity thieves after just a few people are defrauded instead of thousands, data mining will play a critical role in identifying serious crime trends in their earliest phases and in preventing terrorist attacks before they occur. Of equal importance however, is to accomplish these things while protecting the privacy

of the innocent, a function that is possible to design into the technology.

Another important area of information technology research is combining and utilizing data from different media formats. For example, law enforcement data can be in the form of audiotapes or files, surveillance footage and/or, phone records. Technology exists today that can transform those media into formats that can be processed and queried. In addition, much potentially valuable information in the form of free form text is never processed. At most, systems in the past have been able to search those items using keywords. Smart techniques such as entity extraction and natural language processing could be employed to process free form text a priori, extracting meaning and linkages and integrating it with other information. This in turn will require preprocessing techniques, not often used in current law enforcement information systems.


The Power of Networks

The power of technology in the Information Age lies not only in the tools that will identify, track and monitor people and things in our world, nor in the individual tools for gathering, processing, storing and analyzing the data that are generated. Power in the Information Age rests upon the ability of law enforcement officers to act collectively in a synchronized and complementary way, quickly and effectively using information to solve problems before they occur or as they are emerging. Individual officers will need to use the new and powerful tools being developed today and law enforcement agencies will need to process and analyze vast amounts of information and turn it into useful intelligence, but it will be the linking of law enforcement officers with all the information necessary to succeed that will have the greatest impact on the profession by 2015.

The Industrial Age manner of ensuring that members of a group are synchronized and working collectively toward a common goal is to create hierarchies and bureaucracies. Bringing many disparate departments under one organizational umbrella with centralized decision making and a single command and control process is one way to achieve information sharing and synchronization of individual actions and is the traditional law enforcement method of organization. We are continuing in this tradition even as we strive to improve police operations in the 21st Century. There are efforts in some localities to regionalize smaller agencies into larger ones, and at the federal level we have seen the creation of large bureaucracies governing previously independent agencies or the creation of “czars” controlling many disparate agencies in order to mandate their cooperation.

But technology today is creating a new operational paradigm—networks. Pervasive digital technologies are allowing people and information to connect in ways that have never before been possible. Bypassing hierarchical hurdles and tapping immediately into sources of information without the need for bureaucratic process and permission is inherently more efficient than traditional highly structured organizational models (Barabasi, 2003). In fact, in this new Information Age context increased bureaucracy may be antithetical to operating effectively in a dynamic and rapidly changing world.

Our criminal and terrorist adversaries are already beginning to understand the advantages of the network-centric model over traditional hierarchical organizations. Networks foster information flow to and from the individuals those members at the edge of the organization, doing the work that accomplishes a collective mission, and allows them to coordinate their actions without the centralized direction and control that slows



operations and decision making in traditional organizations (Alberts, Garstka 1999). The US military has been developing a network centric warfare model of operation for many years, and we are now beginning to understand its potential benefits within the law enforcement community in the wake of the 9/11 terrorist attacks. The notion of “connecting the dots” and the mantra of “sharing information” are an early manifestation of this network-centric movement in law enforcement, a realization that in order for information to serve a useful purpose it has to be readily available to the right people at the right time no matter where they might be working, regardless of agency or level of government.

Over the next decade a shift toward network centric operations will become a law enforcement imperative as digital devices such as Radio Frequency Identification (RFID), Global Positioning System (GPS), and micro-sensor devices are incorporated into everything and everyone in our communities. As more and more people become “wired” and the individual components of our world are weaved together into “intelligent environments,” traditional business processes will be eclipsed by those that take advantage of networks and their inherent ability to connect people with information seamlessly and immediately. Net-centric policing will be further improved as shared interagency networks, both wired and wireless, are constructed to accommodate multiple agencies from multiple jurisdictions, breaking the arbitrary agency boundaries that have historically constrained the flow of information.


Conclusion

In today’s 21st Century Information Age world the number and types of technologies capable of being applied to one or more aspects of law enforcement is mind boggling. Coupled with

a rapidly expanding definition of what actually constitutes policing in the age of homeland security and the war on terror, the perpetual shrinkage of available resources, and the rate of change technology is bringing to the rest of society, it is easy to imagine civilian police agencies being overwhelmed by events and becoming less effective in the coming years. Developing and implementing the technologies and constructing the networks that will improve law enforcement operations by 2015 will take a concerted and Herculean effort. For a profession that continues to grapple with basic concepts such as combat vs. community policing and the appropriate role of sworn vs. un-sworn crime fighters in our organizations, the issues of Information Age technology seem daunting.

When it comes to improving law enforcement through technology, however, our most important consideration should be the effect that improvement will have on constitutional liberty. While it might be true that another or a series of 9/11-type terror attacks may do as much to damage civil liberties as overly aggressive law enforcement, that should not be a reason for police to willingly disregard the Constitution and use technology in ways that overstep our traditional democratic values. Law enforcement in a free society is only improved when it serves those values while fulfilling its mission to protect the innocent.

At the same time it is also important to remember that the technologies useful for law enforcement in the Information Age are already under development, most of them for military and commercial application. In the face of a growing terrorist and criminal threat to an increasingly vulnerable society these technologies will inevitably be used to stop or eliminate the threat, if not by civilian law enforcement agencies then by someone else. The military and private security firms are gearing up to take on those challenges today and



have the means and willingness to step up to the plate whenever necessary. As technology continues to advance even the general public will have the means to use technology for their own protection.

There is nothing inherently wrong with the military, corporations or the public assisting the civilian police in our collective law enforcement effort. They have been doing so for many years with great success. The danger we face in the Information Age comes from the very significant impact technology plays in our efforts to fight crime and stop terrorism and the threat those same technologies pose toward civil liberties if used inappropriately. Civilian law enforcement is the only organized component in society with a mandate to both protect civil liberties and enforce the law equitably for all people while being trained to do so. To accomplish these equally important objectives it is imperative that civilian police lead all efforts to fight crime and terrorism domestically, coordinating all other agencies and groups, public and private that are contributing to the effort, ensuring that the protection of civil liberties is at the forefront of every action and operation within our communities. If we fall too far behind the military and the private sector in our ability to understand, acquire and use advanced technology, the dominant law enforcement leadership role will shift to those who have the technological capabilities we lack.

References

- Alberts, D., Garstka, J., Stein, F. "Network Centric Warfare: Developing and Leveraging Information Superiority," Department of Defense, Washington, DC. 1999.
- Barabasi, A., "Linked: How Everything Is Connected to Everything Else and What It Means for Business, Science, and Everyday Life," *Plume*, New York, New York. 2003.
- Embley, Paul S: "XML in Justice Information Sharing: An Executive Summary," *Police Chief*, December. 2002
- MacDonald, Heather: "What We Don't Know Can Hurt Us," *City Journal*, Spring.

Policing and Homeland Security in 2015

Richard A. Myers
Alberto Melis

In virtually all crises of national scale, the response of the federal government has been to make funds available rapidly and in large amounts. In the wake of the multiple attacks against American iconic targets on September 11, 2001, that pattern repeated itself. The phrase “Homeland Security” was introduced into the U.S. police lexicon in the waning days of September 2001, to describe both the goal and the rationale for government actions to prevent future attacks. It encompassed a combination of target hardening initiatives, laws and regulations increasing intelligence, and efforts to improve the distribution of information throughout law enforcement, all intended to increase and improve the response capacity of first responders. As part of this effort, the federal response quickly made money available to government units at all levels to invest in technologies, training, and coordination. Immediately, questions began to arise about what role local policing would play in improving homeland security.

History was further repeated when many local agencies within the public safety arena exploited the rapidly disbursed pool of money to acquire items that had been discarded from previous years’ budget processes. As with LEAA funds in the 1970s, millions of dollars have been spent on protective equipment and “toys” that are unlikely to ever see the light of day or have direct applications to the anti-terrorism effort.

Throughout the evolution of the contemporary dominant Community Oriented/ Problem Solving model of policing (Trojanowicz

and Bucqueroux, 1990; Goldstein, 1979, 1990), most police leaders have marketed the activities of their departments to closely match the idealized vision of the model. Such has been the case with homeland security. In fairness, such practices are driven by the financial incentives of (and the strings attached to) the federal money stream. Departments that five years ago were characterizing their proactive efforts and need for technology as COP/POP growth began characterizing many of the same activities in the name of homeland security.

Despite the fiscal motivation of homeland security as a growth industry in policing, there is no universal definition of what homeland security means. Does it contain elements of the old Crime Prevention movement (target hardening)? Is it a way to justify practices that profile suspicious persons? Is it about local law enforcement taking more direction from, and acting subserviently to, the federal terrorist experts? Does it include such daily garden-variety crimes as drug trafficking and domestic hate groups? Is it limited to international efforts to create chaos within the U.S?

While we cannot discern the answer to many of these questions yet—indeed, the answer may be “Yes” to all of them—such variables play into our examination of what the role of policing will be in the homeland security arena in 2015.

Predicting the future with any degree of certainty is difficult. Each action can best be seen as a straight line, and at the choice point it splits into two paths, each of which can split again and again as additional decisions and choices are made. As these lines stretch further and further into the future more and more splits are made which diffuses the end view. We call the events and actions that cause these choice points “wild cards,” and these will play a prominent view in our review.

Examination of Wild Cards:

- *Future Terrorist acts on U.S. soil*—September 11th's multiple-strike acts of terrorism had a profound impact on all of the U.S. society, from the economy to industry to the military, and also inside the schools and homes of all Americans. Support from the grass roots swelled as the president shaped the government's response, including initiating the entire investment into funding for homeland security and the military deployment and attacks against the believed bases of the Taliban and al Qaeda. The realignment of the multiple agencies into the Department of Homeland Security, which moved hallowed and storied organizations such as the Secret Service, Immigration and Naturalization, and the U.S. Coast Guard under a single director, was the biggest and most complex federal reorganization since the end of World War II.

In the earliest days of post 9/11, partisanship was a mere whisper and unity was the theme being espoused from both sides of the political aisle in Washington. However, in the 2004 presidential election, rancor and divisiveness often centered around the war in Iraq and other strategies (or lack of strategy) to continually attack terrorism's roots. While the absence of additional terrorist acts on U.S. soil made it impossible to measure what impact that would have had on the nation's perspective during this political season, it is fair to say that many Americans have settled back into a daily routine that is more concerned about the state of the economy than risk of international terrorism. As the Iraq military deployment continues to yield additional U.S. casualties, Americans increasingly mourn the deaths with questions about the value of the continued deployment. Civil liberties are

defended more strenuously, particularly visceral reactions to military recruitment tactics and the creation of databases from transactions formerly considered private (airline travel, student enrollment information, library use, etc.).

This perspective could be profoundly altered if there were additional attacks that somehow could be linked to the region where military efforts are focused, or the terror networks linked to al Qaeda, the architects of the September 11 attacks. However, the reaction of U.S. citizens would depend on when, how and where the attacks came. The national reaction to the killing of almost 300 U.S. Marines at the bombing of the barracks in Beirut, and the death of 17 sailors in the attack on the U.S.S. Cole, were radically different from the reaction of the bombing of the Murrah Federal Building in Oklahoma City. All were viewed as tragedies, and evoked strong emotions, but neither of the two military triggered the coalescence of a "national will." The casualties of the al Qaeda-sponsored bombings of the American embassies in Africa barely registered; more concern was raised about the perceived tepid response of the Clinton administration. Even the reaction to the Oklahoma City tragedy, which initially was suspected to be the product of foreign terrorists—with civilian victims including infants at a day-care center—was muted compared to the deaths resulting from the World Trade Center, Pentagon, and Flight 93 crashes.

Therefore, future acts of terrorism within the U.S. are significant choice points that will have a profound effect on the nature of policing's role in homeland security. Further refining this "wild cards" is the nature of potential future attacks. Major attacks such as the September 11th scenarios are large in scale and highly visible; nonetheless, they represent single failures of defense in an arena where the odds favor attack. Lesser attacks could be executed more frequently, with less planning and

coordination required, and could increase the sense of vulnerability across the U.S. even if the casualty numbers are smaller. Multiple small-scale attacks imply a widespread failure of the defensive network, symbolically elevate the capacity of the attackers, and increase the national unease. Few of us work in high-profile locations like the World Trade Center, the Pentagon, or the United States Capitol building, and we can take comfort in our relative isolation. But if Smallville and Anytown and the little houses on the prairie are attacked, then all of us are at risk. The nature of future attacks is itself somewhat of a “wild cards.”

Part of the homeland security initiative has been a fairly thorough examination of the strengths and weaknesses of America’s defense abilities. As this chapter is being written in summer 2005, the national headlines bear dismal reports. Almost four years after the 9/11 attacks, our intelligence communities remain mired in turf battles, and major agencies are taking political heat for inefficient response or retooling efforts. The much-ballyhooed technologies are nowhere near being deployed on a widespread basis, and only a few are at a stage of development where they can be considered useful. The contributions of private entities are being questioned, from Iraq to airport security, and we are acutely aware of the vulnerabilities of our seaport facilities to infiltration. The language of attack now includes a constellation of nuclear, chemical, and biological weapons: black-market nuclear weapons from the ill-guarded arsenal of the former Soviet Union; “dirty bombs” of conventional explosives that spread radioactivity from a growing catalog of missing nuclear material below weapons-grade quality; anthrax, ricin, ebola/Marburg, plagues of various, cyber attacks on the nation’s power grid and other infrastructure targets.

Each one of these dangers, set in the multiple possible high-profile targets where they could be

unleashed, taxes the capacity of first-response agencies. Each requires specialized equipment, contingency plans, articulated agreements among government agencies, NGOs (Non-Governmental Organizations) and private providers, and an enormous amount of time devoted to planning and preparing for events which may not happen. “Readiness fatigue” is a constant danger, with each elevation of the national color code constituting a cry of “Wolf!” that Aesop surely would recognize, if glumly.

- *Traditional Street Crime:* Throughout the 1990s, the U.S. in general saw declines in street crime in most regions. Without addressing the potential reasons for the declines, such as the youth cohort in “prime crime years” or the impact of the federal COPS (which again, distributed large amounts of money to local agencies), the next decade *could* see increases in street crime that would adversely affect quality of life in American communities. With many local communities and states grappling in the mid 2000s with budget deficits and shrinking resources coupled with pressure to hold or reduce taxes, there are limits to local policing’s ability to hold the lid on street crime **and** become the front line of homeland security. The nature of the crime rate will likely affect the role of policing in homeland security in 2015.
- *Crimes of the Future:* The very nature of crime is a “wild card” for 2015. In the late 1990s, police had never heard of phishing and spoofing. Identity theft was in its infancy and largely consisted of stealing identification cards rather than the whole identity of the person. What will the new crimes of the late 2000s be? The resources needed to investigate future crimes that we

don't even know of today will likely shape the role of policing in homeland security in 2015. Many law enforcement agencies have added computer crimes to the specialized units that they have, and struggle with the cost of keeping up with those mandates. Those imperative and resulting costs in keeping up with the technology are continuing to change.

- *Nature of International Relations:* Could the next decade be another of the recurring Age of Reason periods of history? Historically, insurgencies don't last forever. People tire of constant killing and violence. In 2005, historic hotspots of violence and terrorism from the 20th century have calmed significantly, e.g. Northern Ireland, and there is a fragile but hopeful dialogue between the Israelis and the Palestinians. We are seeing this in Spain as every action by ETA is met with increasing public displays not against the government (itself not a well loved institution) but against ETA. The feared Baader-Meinhoff gang in Germany is extinct, as is the Brigatti Rossi in Italy, and the Red Army Faction in Japan. The Sendero Luminoso in Peru and surrounding countries is marginalized, and there are on-again, off-again negotiations in Colombia. There is no reason to believe that the same will not happen to other insurgent groups throughout the world.

The emergence of the World Court at The Hague as an international center for resolving local war crimes disputes (despite American refusal to approve the Court) provides promise even as local disputes continue to flare in Aceh, Darfur, the Ivory Coast, Nepal, and elsewhere. While the current adjudication of war crime allegations from Bosnia, Rwanda and Darfur do not hold the same fascination

as the Nürnberg prototype following World War II, there is a greater awareness of world standards that may be applied to new conflicts in more timely fashion. The Group of Eight and the World Trade Organization are dealing openly with the issues related to African poverty. Border-spanning issues such as AIDS, drug patents and government subsidies of airline industries are moderating the older fixation on the supremacy of the nation-state.

The resurgence in fundamentalism in the Islamic world is also reflected in the United States, but not in Europe. European attendance at churches is at an all time low (prompting the late Pope John Paul II to urge formal recognition of Europe's "Christian character and heritage" in the Constitution of the European Union). The fastest growth in Catholicism is occurring in Latin America and the African subcontinent; the greatest religious growth in the United States is evangelical in nature. These currents will change not only our understanding of world events, but how the world views us as well.

There is also an economic renaissance elsewhere in the world. The European Union is increasing in economic force by leaps and bounds, despite the constitutional crisis of the French and Dutch "no" votes. A resurgent China is becoming an enormous purchasing and manufacturing power, as is India—and they are expected to outspend and outpace the United States in terms of oil, thus driving the price up. This will have a profound impact in our economy and our sphere of influence.

- *U.S. Politics:* While the political system itself to some degree reacts to the above-mentioned "wild cards," it contributes to the uncertainties. Changes in the presidency and the overriding philosophy affect the role of federal government in relationship to locals. Typically, the pendulum swings to and fro. We are undergoing a period where politics

are less introspected and tend to be more concerned with our sphere of influence. This was exacerbated by the 9/11 attacks. Other administrations and parties have been more concerned with internal policies and less with external influence.

At this point in time, the administration's formerly solid support within the houses of government appears to be waning. Support for the foreseeable short to middle term will be affected by the wild cards outlined below. There will be another election in 2006, and in two years after that—and both those elections will be very much influenced by the public's perception of what goals have been met, and how deeply we are still involved in a war. In fact, the elections may very well be decided on just those two factors.

While the Supreme Court is generally thought of as above the rough-and-tumble of politics, its decisions also affect the actions of state and federal entities. In its most recent session, the Court has appeared to be more receptive to federal powers, reversing what had been a states' rights character for most of Chief Justice Rehnquist's tenure. Whether that is a product of the climate of homeland security or merely a parallel phenomenon, the strengthening of federal power supports and may even encourage stronger centralization control. The resignation of Justice O'Connor and death of Chief Justice Rehnquist in 2005, and the subsequent confirmations of Chief Justice Roberts and Justice Alito will surely affect the balance within the Court on important issues.

- *Influence of the Media:* As the Internet becomes more ubiquitous; the role of the media may decline. Blogging is increasing, while the traditional major network television news departments are viewed with less importance. Dan Rather's

unceremonious departure from CBS News in 2005 reflects the consequences of competition-driven "fast news" instead of well-researched journalism of the past. The 2005 brouhaha over "video news releases" masking government positions under the guise of independent news, the direct federal sponsorship of particular stories (and at least one set of White House media credentials) further weakened the public confidence in the media, albeit from the other end of the spectrum.

Peer-review accountability of blogs may hold increasing appeal, and the availability of Internet access equals or exceeds global access to satellite fed television. With growing information and news the relevancy of traditional media is an unknown wild card, as is the influence of whatever may take its place. "Niche news," preaching a particular position to an already-agreeable audience, is a far cry from the iconic "free press" that questioned government with an independent mind. Nor is it clear that freelance blogging represents an improvement; history has yet to judge whether the bumper crop of political bloggers are the Benjamin Franklins and Horace Greeleys of the Internet, or mere poseurs with little more to contribute than the drunk in the corner bar.

From this examination of "wild cards," a continuum of paths models emerge on what policing in the role of homeland security could look like in 2015. At one extreme of the continuum is the environment of war; this model would look highly militaristic, authoritative, with little concern for civil rights. The other extreme represents an evolution of policing that reflects its path pre-9/11; this post-reform COP/POP would be a peacekeeper model, mostly focused on sustaining community quality of life, with high sensitivity to civil rights and social

concerns. In the middle, we envision an “adaptive” state of policing that is situationally driven; this might include a wide base of skills, training, and leadership modalities that allow police to shift between the extremes depending on demands from the environment.

The War Model-2015

A militaristic, low civil rights, high authority model

(War based Homeland Security model)

In the War Model of policing’s role in homeland security in 2015, police officers are mandated under federal law to verify identification from the national ID database. Street patrol officers carry the technology on foot and in patrol cars to verify instantly the information contained on the mandatory national identification card. If officers come in contact with someone without their ID, they obtain and submit the individual’s fingerprints into the national AFIS system, where full ten-fingerprint sets of all American citizens and legally admitted visitors are archived. They also submit a digital photo of the person’s face for image recognition software to verify from the national database.

Local police officers have been given federal authority to take unverified persons into custody. People whose identity cannot be ascertained on the street are taken into civil custody pending identification. Absence of a verifiable ID is a federal offense; however, local counties are required to make detention space available. The unfunded mandate places considerable strain on urban jurisdictions, and there are rumors of covert non-feasance in immigration enforcement by municipal agencies. Old-style cultivation of community-based intelligence continues unabated, with an occasional nudge and sly wink underneath the tough “homeland

security” rhetoric in public speeches.

Libertarian objections to “Seine papiere, bitte!”—a deliberate invocation of the Nazi occupation of Europe—were eviscerated by premature and over wrought comparisons of the Guantanamo detentions to the Nazis and Pol Pot regimes, and by a rash of nick-of-time apprehensions of false-document infiltrators seeking to plant explosives at sensitive points in the nation’s power grid. As the generation of Holocaust survivors and their liberators died out, the rhetoric of “protection” was joined with concern over the problem of identity theft to produce a pluralistic consensus in favor of mandatory national identification

Despite past protests of the nation’s chiefs of police and sheriffs, local law enforcement now manages about 60% of the enforcement of immigration laws. Local officers are also required to leave their jurisdiction to assist other agencies in the event of a terrorist act, as so declared by each State’s Office of Emergency Management and Terrorism Response.

Due to continued budget challenges following the nation’s ongoing military efforts globally, the Department of Homeland Security provides direction to the states’ Offices of EM and TR. Like the 75-50-25 funding of the COPS grants, the federal largesse faded in the wake of continued military presence in Iraq, Afghanistan, Indonesia, the Philippines, and Nigeria, and the collapse of the medical insurance industry. DHS has shifted many of its duties to state, regional, and local agencies. In the major cities, local police conduct harbor searches, operate regional intelligence centers, and provide baggage and passenger screening at local airports. Initially funded by rounds of DHS grants, the expense was shifted equally to travelers and to local communities. Many of the staff are civilian employees who represent a much larger percentage of the policing workforce. Privatization has shifted

some of the tax burden, with local authorities retaining nominal control over private security actions. Nevertheless, the long-standing concerns about the quality of private security remain salient, and there are episodic scandals, commissions and reports that gather dust on the shelf.

The proliferation of public surveillance cameras has shifted from being exclusively urban to suburban to regional, having not yet penetrated rural areas in any systematic way. Dummy cameras have replaced faux alarm company stickers as the cheap crime-prevention ploy of choice in rural areas. All locations housing explosives, precursor chemicals, or potentially dangerous electronic equipment are under round-the-clock CCTV monitoring and access control, and many private farmers and ranchers use localized CCTV, monitored in their houses and from their PDAs.

Police no longer need search warrants or permission to simply tap into the streaming video feed and blend with public cameras. Software controlling the cameras identifies patterns of behavior thought to be “suspicious” or that pose a threat to the national security. When the software triggers such a pattern, police need no further justification to stop and demand identification. The ubiquitous police-monitored urban cameras are interfaced with the existing archipelago of private security surveillance cameras, creating an integrated real-time tracking network.

Similar software is integrated with the circulation software of all libraries, municipal or academic. Patterns of materials that are checked out that meet the “threat to national security” profile trigger identification through the national ID card used to check out materials and the video surveillance images. Internet surfing tracking software has been in place for a while, but the creativity of technology hobbyists makes it less reliable. Parental controls for cable channels have

been replaced by governmental filtering that cuts off programming of a subversive nature.

Basic police academy training has skyrocketed from the 8-15 weeks of a decade ago (2005) to more than 9 months. Recruits attend training in six-week increments, and then rotate through a series of “practicums” including security roles (airports, harbors, etc.), Emergency and Terrorism Response Teams (ETRTs), crime scene assessment (hazardous materials, secondary device awareness, etc.). Civilian police employees who handle most of the support and technical roles (intelligence, crime analysis, evidence processing, etc.) go through specialized training at regional and national sources e.g. the FBI Academy.

One contributing factor to the lengthy extension of training time is the need to prepare officers for instant “shoot-don’t shoot” decision-making. In the first decade of the 21st century, police were restricted by the requirement of imminent threat of death to the officer or another before authorized to use deadly force. With the growth of Improvised Explosive Devices (IEDs), officers are now trained to closely observe behaviors and appearance that are indicative of an imminent terrorist act. Officers are under order to immediately send streaming playback video of what they observed for computer analysis, and can receive a “shoot to neutralize” order based upon this analysis. Officers working in high-risk areas (major cities and Standard Metropolitan Areas [SMAs], jurisdictions with high-profile infrastructure targets, and border assignments are under particular scrutiny in this regard) receive weekly training and assessment on their ability to apply the dual standards for use of deadly force.

Beyond local police officers and county sheriffs and state police, regional divisions of ETRTs are deployed strategically across the nation. They are available to be flown into a hot spot area, and

assume a heavy combat role in the event of major situations. These units are not under the command of the local chief or sheriff if deployed, but fall under the command of the quasi-military Department of Homeland Security structure within the federal government. They are virtually indistinguishable from the global U.S. military except for their uniforms, which are all black.

The ETRTs have a local and regional component, more closely aligned with local law enforcement, that provide the backbone for the major staffing of security at major events such as sports stadiums. What required 100 officers to police back in the early 2000s now requires almost 1000. Screening for dirty bombs, IEDs, and any other type of weapon is done through a blend of private security and heavily armed police.

The use of civil commitment has been expanded beyond its original application to the criminally insane and dangerous sex offenders. A right-wing attempt to repeal the 14th Amendment's provision of "nor deny to any person within its jurisdiction the equal protection of the laws" failed, and the internment center at Guantanamo Bay closed in the face of international opposition. In response, the United States Code was enhanced to allow for the indefinite civil commitment of persons meeting a certain evidentiary threshold of connection to terrorist groups defined by Congress. Under the Enterprise Theory of Crime, RICO statutes extended eligibility to groups otherwise classified as street criminals if their activities were linked to proscribed terror groups. Several street gangs, including one outlaw motorcycle club, were removed from the streets to the new Maximum 7 security prison on the outskirts of the former Area 51 research center in Nevada

The Peace Model:

A post-reform COP/POP Model (Peace based, more traditional police role)

With the remarkable absence of additional attacks by international terrorists on U.S. soil, the role of policing in homeland security in 2015 can be described as fine-tuned but not significantly changed from a decade earlier. Major cities and high-risk targets sustained a level of high vigilance, fiscally supported somewhat by the federal government. But at the local level, the degree of attention spent on homeland security is partly driven by the local political climate. Fiscally conservative communities accustomed to stable crime rates and high quality of life invest their tax dollars on core, basic services, keep the tax levy low, and provide a full range of social services. Urbanized areas that have long required a heavy police presence soften the burden of a significant police investment by linking the expenses to resource streams that support Homeland Security.

After the U.S. significantly reduced its military presence in Iraq and global insurrections seemed to calm, Congress engaged in lengthy debates on the original Patriot Act, examining the many concerns expressed throughout the 2000's. Some of the powers originally granted were kept, but required a higher level of judicial review and were severely limited in the scope of their applicability. Contrary to what some predicted might happen, massive consolidation of the thousands of police departments nation-wide didn't occur. The notion of "local control" remains, and local police activity reflects this philosophy.

Some communities, again usually those with higher crime rates, have mirrored the private sector's use of surveillance cameras with deployment of ubiquitous public cameras. Local police

accountability boards (PABs) closely scrutinize the police use of such “big brother eyes.” Likewise, the PABs review citizen complaints on excessive use of force and threats to civil rights, as the public dialogue on issues like racial profiling evolved into a reiteration of the U.S.’s foundational civil rights. Geographically defined Neighborhood Policing committees provide direction and priorities for neighborhood beat officers (Futures Working Group, 2005). In communities that demonstrated deep commitment to the 20th century construct known as Community Oriented/Problem Solving Policing, police leaders concluded that the best form of homeland security was a total partnership between the citizens and police, engaged in sustaining the local quality of life. High percentages of residents in such communities have been trained by their police on how to take ownership of their neighborhood’s problems and be part of the solution. Volunteerism is a key resource for local police departments, as the cost of providing sworn officers is high. Civilian support staff increasingly manages tasks formerly mastered only by officers.

While the federal government provides support funds on a very limited basis to local agencies, to qualify, policing must comply with the National Incident Management System that was promulgated in the mid-2000s. Police, fire, public health, public works, and most other municipal service workers are fully trained and can readily fall into an Incident Command scenario, with shifting Commanders depending on the current focus of the incident. Ultimately, the local unit of government maintains control of its resources and is “in charge” unless it hands-off control to a regional or state Emergency Management resource.

In the decade between 2005 and 2015, technology related crime increased exponentially. Identity theft became one of the most common criminal acts, but went largely unprosecuted because

of the challenges of the global jurisdictional issues. Interpol eventually assumed a coordinating role on all technology crimes that cross national boundaries, with world “computer courts” that would adjudicate global offenses. With the aging of the U.S., criminal behaviors were evident in older offenders; aging criminals who would forego street crimes in their twilight years found stealing through a keyboard an age-friendly practice. With women’s role in American society equaling men’s, an increase in women offenders required investment in women prison infrastructure. Prison populations in general dropped by the increasing use of monitoring technologies and restorative justice methods.

Police use of technology varied; well-funded communities with more substantial population density invested in emerging technologies and collaborated through regional or national efforts, such as AFIS and digital image databases. Analytical software and networking of police information systems with access to palm-size devices were standard in such communities. Small towns faced difficult decisions: either disband and be absorbed by regional departments that could provide such technologies, or continue in providing familiar services with severe economic constraints.

Whether small or large, local policing with local control does not preclude a networked infrastructure. A national grid of information system nodes is made available to any and all law enforcement. For fees based on community size and demand, analytical services and intelligence are provided by a consortium of government and the private sector. Security is high, but the notion of public/private partnerships is well established by 2015.

Over the last ten years, police training has changed with technology. The use of Virtual Reality (VR) and Augmented Reality (AR) have created extremely effective simulation training that better

prepares officers to apply the full range of police tactics, including use of force and rapid identification of criminal behavior patterns (Cowper and Buerger, 2003). Basic recruit school has lengthened to incorporate more scenario-based and simulation training, and in-service training has both state and federal mandates for minimum standards.

The Adaptive Model

In the middle, an Adaptive Model that is situational; wide base of skills, training, leadership modalities that allow police to shift between the extremes depending on the environment (might require flexible work-staffs, deployment of the warriors to augment the locally based peacekeepers).

By 2015, the U.S. had endured additional terrorist acts, but none were close to the magnitude of September 11th. IEDs occasionally went off in public places, but the American culture resisted their promulgation to the level seen in Israel in the 2000s. A dirty bomb attempt resulted in debilitating injury to the bomber, but only a handful of innocent victims received sufficient contamination to trigger health issues. Most common were acts of sabotage upon the country's critical infrastructure, which managed to inconvenience many people until corrective actions were taken. The role of the police, in turn, incorporated the vigilant protection of critical infrastructure and the rapid response to covert or overt threats, as they became known.

Under federal mandate, police nationwide were expected to be skilled and capable in Incident Command. The federal government subsidized statewide ETRTs, which were a blend of full-time state employees, augmented by specially trained local officers who were obligated to respond if the ETRTs deployed. A joint Incident Command system with local and state control applies whenever these teams are deployed.

The nationally standardized ID card is subject to mandatory carry laws under the terms of the "Patriot Law", a domestic version of martial law implemented under times of great threat of attack against U.S. soil. Provisions of the old "Patriot Act" were modified into actionable requirements that provide sweeping powers for police during periods of "Patriot Law". The president must obtain concurrence from the Congress to invoke "Patriot Law," and as of 2015, it has been used sparingly. Civil liberties that are restricted under such challenging times have been the subject of intense debate and protest. The Supreme Court has been weighted down with countless cases seeking what possible constitutional language can justify the extreme measures that many Americans support during times of duress.

States have adopted the national standards for driver's licenses and state issued ID cards, with a nationally accepted method of easily capturing data from the card for verification.

Publicly employed police officers, while fewer in number than their private sector counterparts, have become highly trained with a varied mission. During typical times, they continue to work with their communities to mutually solve problems and improve quality of life, but they also maintain a skill set of combat when needed. Special squads with exclusive combat methods are available to move into high-risk areas. This resource resembles the military, with whom the police share a training and deployment relationship. During "Patriot Law" times, the military is authorized to jointly operate with combat police units. Every police officer spends at least a year in training and rotates through the many special skill areas within departments.

One contributing factor to the lengthy extension of training time is the need to prepare officers for instant "shoot-don't shoot" decision—

making. In the first decade of the 21st century, police were restricted by the requirement of imminent threat of death to the officer or another before authorized to use deadly force. With the growth of Improvised Explosive Devices (IEDs) officers are now trained to closely observe behaviors and appearance that are indicative of an imminent terrorist act. Officers are under order to immediately send streaming playback video of what they observed for computer analysis, and can receive a “shoot to neutralize” order based upon this analysis. Officers receive weekly training and assessment on their ability to apply the dual standards for use of deadly force.

There is significant staffing of security at major events such as sports stadiums. What required 100 officers to police back in the early 2000s now requires almost 1000. Screening for dirty bombs, IED’s, biological agents, and any other type of weapon is done through a blend of private security and heavily armed police.

The U.S. government distributes funding for major anti-terrorism police efforts and terrorism prevention in the communities that either have been identified as having the highest risk, or that have previously experienced a terrorist act. The practice of the early 2000’s to “share the wealth” among all communities proved inefficient, as many items purchased were never deployed or needed, while other communities suffered from basic protection. To correct the past efforts of local authorities to lump any and all criminal activity as “terrorism” to qualify for funds, the federal government has established clear parameters that require a direct link to either global or domestic terrorist groups before qualifying for funds or classifying as “terrorism.”


The military’s authorization to deploy with police is not strictly limited to “Patriot Law” situations. In 2015, local mayors have the ability to

request through their state’s governor deployment of both National Guard and regular military to augment local law enforcement. While the standards for such deployment remain extraordinary, the lines between policing and the military have become blurry.

In 2015, there are many more private police than publicly employed officers. Communities with resources have outsourced much of the service mission of policing to private enterprise, often in conjunction with gated entrances and walled neighborhoods. While standard patrol activities continue in many places, the amount of residential space for which the public police are responsible has shrunk, and responsibility delegated to private and special-jurisdiction forces. Wags refer to them as “the police reserves,” since many of the private officers still aspire to public police careers despite considerable evidence that wages and benefits are better in the private services. The subcultural consciousness still has not shed the mystique of “the real police” that attaches to those with broad rather than limited police jurisdiction.

While some described policing as a growth industry, it was well below the pace of private security moving into 2015. One of the new police powers allows for police takeover and command of private policing and security enterprises when Patriot Law is invoked. The first such attempt was widely acknowledged to be a disastrous circus of the absurd, with many parallels drawn to the Keystone Kops of old. The practical result of that first failure was a series of DHS-sponsored joint training activities similar to the old Incident Command process. Greater preparation for mobilization under national emergency has yielded a much greater degree of public-private coordination in standard crime control.

With fewer disposable federal dollars, but increasing demands on local agencies, regional



efforts to consolidate police departments have had mixed results. In some areas, one large agency evolved from several smaller. In other areas, the decentralized delivery of police services was possible through centralizing the support services that are transparent to customers. Most communities have recognized the need to sustain local control over typical police operations, but also understand that the times of “Patriot Law” call for diverting some control over to a more centralized authority. As has been true throughout police history over the past 100 years, the burden is ultimately placed

on the neighborhood beat officers to develop the relationships needed to balance freedom and law.

References

- Cowper, Thomas J., and Michael E. Buerger, 2003. “Improving Our View of the World: Police and Augmented Reality Technology,” Monograph published by the Behavioral Sciences Unit of the Federal Bureau of Investigation for the Futures Working Group collaboration, Quantico, VA. February 2003. Also available at: < <http://www.fbi.gov/publications/realitytech/realitytech.pdf>.>
- Futures Working Group, 2005. “Neighborhood-Driven Policing. Proceedings of the Futures Working Group, Vol. 1,” Monograph published by the Behavioral Sciences Unit of the Federal Bureau of Investigation for the Futures Working Group collaboration. Quantico, VA. January 2005.
- Goldstein, Herman, 1979. “Improving the Police: A Problem-Oriented Approach,” *Crime & Delinquency* 25, 236-258.
- Problem-Oriented Policing*, Philadelphia: Temple University Press, 1990.

On the Horizon: Police Training in 2015

Joseph Schafer, Sandy Boyd & Alan Youngs

Introduction

Training, by its very existence, is subject to constant review and assessment. In no other profession is this more pertinent than in law enforcement. Consider the following excerpt from an article on police training:

The role of the police officer can not be minimized, and in these days when the complexities of human relations have been greatly increased and tensions are encountered beyond those known in former years, it is essential that the police officer have the finest... training possible. We cannot afford to take chances in this regard.

The quality of a police force and its degree of professionalization necessarily depend upon the effectiveness of its training program. The keystone of modern progressive law enforcement is the police-training program.¹

Today this passage seems commonplace, which is not overly surprising considering the strides that have been made in law enforcement since the 1967 President's Commission Report. However, if you consider the date this was written—1957—it emphasizes that what is now accepted and expected practice was considered innovative and progressive 48 years ago. We have come a long way in police training, but we still have a long way to go.

Law enforcement officers face a wide variety of complicated and dangerous situations on a daily basis. Any set of circumstances that may be complex or routine, innocuous or deadly, may occur at any moment. With each passing year, criminal behavior

and methodologies continue to evolve; likewise, the practice of detecting, investigating, and responding to criminal behavior also changes as techniques are developed and refined, laws are modified, and technologies emerge. All of this requires that police officers possess a wide range of interpersonal, physical, and mental skills, knowledge, and abilities.

Over the years, all levels of law enforcement training have been delivered in a traditional style, with instructors lecturing to a classroom full of students on skills training, legal training, and internal notifications (e.g., changes in policy and procedure).² The limited time spent on practical applications was restricted to areas such as weapons training, where the trainee was able to develop only a certain level of proficiency with a weapon. Unfortunately, this did not provide the needed judgmental training and experience in dealing with critical, stress inducing situations involving possible use of lethal force. Beyond the issue of use of force decision-making are the day-to-day realities of policing in today's world. As "threat assessment" has become an everyday part of our language, modern-day policing demands a greater awareness of a broad array of topics, and more practice is needed in making decisions in diverse areas beyond the deployment of force.

Ideally conceived, police training accomplishes the same goals for two groups of officers. For new recruits (pre-service) and established personnel (in-service), training is supposed to enable officers to receive, process, and act upon information in an effective manner. This holds true in all realms of policing, from the use of force, to the decision to arrest, to the handling of distressed individuals, down to the issuing of a parking ticket. Regrettably, much police training (both pre-and in-service) continues to rely on lecture-based instruction, rather than exploring other educational modalities aimed at establishing and

developing good decision making abilities.

In the early 1990s, research on applied learning theory conducted at the Naval Pilot Training Center demonstrated that classroom instruction using visual aids and handout material will cause attentive adults to retain 50 percent of the instructional content presented. If trainees could then personally experience and practice realistic applications of the learned skills or knowledge, the retention rate had the potential to reach 90 percent.³ Military studies revealed that readiness to respond properly during critical incidents was improved when personnel had access to, and occasional use of, practical application training techniques.⁴ Other studies have also shown that the more realistic the training, the better the officer's retention and therefore, at least potentially, the greater their performance and survivability.⁵ The move toward more effective training took a huge leap with interactive video, a technology now seen at most police training facilities. This innovation has filled the void between practical skills training and actual experience in the many skills needed for law enforcement.

The ultimate purpose of any officers' training is to save lives and enhance the efficacy of policing. This is achieved by helping officers better understand policies, procedures, and methods that will enhance decision making and the delivery of policing services. With the addition of modern technology to the training process, this purpose can be better and more effectively achieved. In the contemporary era, training has begun to evolve beyond lecture-driven instruction and limited (and often unrealistic) scenarios. In the future, emerging technologies have the capacity to revolutionize when, where, and how police training occurs. These changes are not decades down the road; rather, many of the core technologies are already being developed. This chapter considers how technological, social,

and management practices are likely to change in the coming decade.

Education and Training

Education and training are fundamentally different, though in an ideal world they should complement each other. Education should prepare a student to succeed in any training regimen or philosophy, or in any occupation regardless of major. The process of education is less a transfer of fact or philosophy than of the skills of learning how to learn. A college education is designed to build within each student the ability to critically assess new situations, undertake new learning as needed, and even to question the "facts" and underlying assumptions of existing canons of knowledge, when necessary.⁶ Training is a systematic building of particular skills, knowledge and abilities that transfer directly to the worksite. Training helps an officer understand the "tools of the trade," such as applying state laws, using defensive tactics, and knowing how to de-escalate conflict situations. It is what an officer "falls back on" in high stress situations. Training curricula also contain a growing number of topics that embody a learning component quite different from wristlocks and takedowns. Domestic violence and child abuse, multicultural issues, legal rights of the accused and other topics too numerous to list now require documented training.⁷

There are several other dimensions that distinguish higher education from police training. Higher education tends to be more broadly focused and more time spent analyzing and discussing materials; training tends to be directed and subject to less critical analysis and debate. Higher education is usually delivered by instructors with formal education exceeding the average levels held by the students, although these instructors may lack job-related experience in the field for which students are

preparing. Training is delivered by instructors who have more job-related experience than the students, although these instructors may hold lesser academic credentials. The evaluation of learning is sometimes the same (e.g., objective examination questions), but is often broader and multi-modal in higher education settings (e.g., increased reliance on the assessment of more abstract notions, such as critical thinking and analysis).

Ideally designed, higher education prepares graduates to succeed in a range of occupational settings because they have learned to learn. Although graduates may still need to acquire the knowledge, skills and abilities of a particular occupation, they are thought to be well prepared to thrive in their professional life because they have developed stronger reading, writing, analysis, organization, and personal skills. Training, in contrast, is intended to simply teach the “graduate” the technical skills required to perform a particular job, such as being a police officer; the skills acquired through training often do little to prepare the graduate to thrive in other occupational contexts.

Educational and training processes are reciprocally linked for many employees. This is especially true in career fields such as policing, where it is common for employees to enter with some level of higher education (e.g., beyond a high school diploma or equivalency degree), to complete the occupational training, and to further their education at a later date (through the completion of a college degree). In the future, emerging technologies and modes of training and education will enhance this situation. In the next decade we will see training become more flexible, customized, and on-demand; higher education will also advance in these areas, although perhaps to a lesser extent. This article will focus primarily on police training, but it is expected that education will continue to advance in a similar fashion. Many observations contained in this chapter

will apply to both the worlds of higher education and police training. In some cases, the boundary between these two worlds, which has always been permeable, will become increasingly blurred.

Police Training, 2005

Although the goal of police training has changed very little over the years, the subject matter has expanded and the modalities used to deliver that training have evolved. The subject matter continues to be reviewed, enhanced, and rewritten in response to emerging crime and safety concerns, changing laws, new insights into the nature of society and human interaction, and shifting views on the “best practices” in policing. Efforts are still being made to increase the professionalism of instructors by requiring a combination of education, time in service, and preparation through coursework and practice in teaching and training.⁸ Academies are seeking subject matter expertise first and then training the instructor to transmit that expertise to the trainees. In many cases, instructors are not allowed to teach until they have completed a basic course in instructional skills.⁹

Since 9/11, an additional charge was made to law enforcement, which added the responsibility of homeland security and at this point is still being defined. Among those changes are a need to be aware of substantive changes in responsibilities and procedures (as the Department of Homeland Security consolidated the efforts of many disparate and formerly autonomous agencies), changing emphases, and the rapid proliferation of critical technologies. Greater coordination with asset protection capacities in the private sector is finally being discussed as an emerging need in police training.¹⁰

Basic academy training varies in length from state to state, and within each state, from

department to department. On average, however, state and local police recruits complete 720 hours of pre-service training, exceeding minimum state training mandates by approximately 100 hours. Approximately one-half of these training hours are focused on a small number of topics, including: firearms skills, health and fitness, investigations, self-defense, criminal law, patrol procedures and techniques, emergency vehicle operations, and basic first-aid/CPR. Approximately one-third of academies include a field training component in their curriculum.

Because of past research, trial and error, and civil litigation, the modalities of police training have a new look. There is still a huge dependence on a traditional lecture format for most material, with a strong reliance on objective examination as the preferred mode of assessment. Beginning in the basic academy, however, there is more opportunity for the trainee to learn, and to prove that learning in different ways. Academies have begun to assess recruits based on other testing formats (e.g., essay exams, written assignments, performance in scenarios and simulations, etc.) and other forms of evaluation (e.g., “supervisory” assessments conducted by instructors and “peer” assessments completed by other recruits).

Technology is also increasingly used to facilitate instruction and assessment in academy environments. Examples of this include:

- Advanced technology classrooms that allow for computer-aided instruction and may offer students access to computer networks.
- Shooting simulators that place trainees in mock scenarios to assess judgment, policy comprehension, reaction time, and proficiency.
- Video scenarios and interactive video programs that place trainees in other types of mock situations to assess knowledge,

judgment, policy/law comprehension, and skill.

- Self-paced tutorials designed to facilitate learning outside of traditional classroom environments.

In-service training also varies nationwide, running the gamut from no hours required (found only in a few isolated and generally poverty-stricken jurisdictions) to a rough average of 40 hours a year, including firearms proficiency. Since 2001, a major expansion of in-service training has come not from state or local mandates (which remain restricted by local funding capacities), but from the federal Department of Homeland Security. Periodic training updates and coordinated-mobilization exercises currently constitute a sizeable proportion of in-service police training activities.

Professional development remains largely ignored in most areas. Officers are left on their own to prepare for transfer, promotion, and other aspects of their career development. In most jurisdictions, this is true both before and after an officer has obtained a promotion or special assignment. Officers are left to rely on informal mentoring from co-workers and peers as they pursue career advancement and acclimate to new job-expectations and demands.

Police Training, 2015

This segment takes a slightly different stylistic approach in communicating the state of police training in 2015. This is the first person story of Sergeant Melina Grace, a fictional officer in a fictional agency, the Youngsville Police Department (YPD). Her experiences and observations are likely to mirror those of many officers entering policing in the current era. Grace was hired by the YPD in the spring of 2005, graduating from the YPD academy in the fall of that year. Grace worked

in the patrol division for the next four years and was then promoted to corporal. In 2012, she had the requisite minimum of five years of service to apply for promotion to the rank of sergeant, and her dedication, work ethic, and leadership ability were rewarded. Sgt. Grace was a shift supervisor in the patrol division from 2012 until 2014, when she requested and was granted a transfer to the YPD academy as an instructor. As an academy instructor, she is involved in training both new and seasoned officers. She has served in this capacity until the present day (2015) and she is currently beginning the process of seeking promotion to the rank of lieutenant.

What follows is from Sgt. Grace's journal on March 4, 2005. Through her eyes and experiences, we explore the state of police training (both pre-service and in-service) in the year 2015.

March 4, 2015

It's difficult to believe that a decade has passed since I was hired by the Youngsville Police Department. Ten years ago today, I entered the academy as a wide-eyed college graduate. In 2005, when I first entered the police academy, we were all impressed and proud to be part of the new wave of policing for the Youngsville PD. After 9/11, law enforcement at all levels of government turned to the training function to better prepare us to not only preserve the public's safety, but to further that mission by ensuring our citizens' security. Now, I stand before a new generation of wide-eyed "kids" and I'm responsible for ensuring that they leave this facility with the knowledge and skills to protect and serve Youngsville. I also stand before my peers (and my mentors) and try to transmit knowledge and skills that will help seasoned officers better protect and serve in new and enhanced ways. New ideas about training and new training technologies have also changed the experience for both new and old

officers. We have moved well beyond the standard lecture-driven training that still dominated when I came on the job.

In some ways, the new recruit classes I see today are not all that different from the officers who were in my academy class in 2015. Almost fifty years after various federal commissions recommended that all new police officers be required to hold a four-year college degree (a recommendation that was supposed to have been realized by the early 1980s!) and nearly a century after August Vollmer helped establish the academic study of criminal justice, college education is still not a universal requirement.¹¹ Sure, some states have been requiring various levels of education for decades and many departments have exceeded those state standards. For example, although my state only requires a high school diploma or equivalency degree, YPD requires that all applicants must have completed sixty credit hours. The reality, however, is that higher education is still not universally valued as a prerequisite for a career in policing.

Although education is not universally required in policing, informally it continues to be important to many agencies. All else being equal, most agencies will take a college-educated applicant over a high school graduate. Education also continues to be important for career advancement. More progressive departments are continuing to adopt standards for the minimum educational level required to seek promotion, with successively higher expectations for higher ranks. More and more agencies are also offering educational incentives, paying officers nominally greater salaries based on their level of education. Fortunately, these trends occurred around the time college programs have begun to do more to cater to non-traditional students seeking to balance work, family, and their education. Although it's still a "buyer beware" market, current officers have a lot of good options that will allow

them to further their college education while still working their job and raising their family.

Education is not, of course, a panacea. There are fabulous cops who dropped out of high school, later earned their GED, and never attended further schooling beyond what their department mandated. At the same time, there are cops with graduate degrees who are lazy, incompetent, corrupt, and all-around poor employees. Education does not make someone a good cop, and the absence of formal educational experiences does not mean someone is a poor cop. That having been said, being at the academy for the last year has taught me something about college-educated cops. As a group, they tend to be better thinkers; they are more analytical, they are better at writing and time management, and they are more aware of the cultural concerns and current events (at local, national, and global levels) that are so important to policing and homeland security in 2015. People have been talking about the intangible aspects of education for decades, and they really seem to be true. YPD requires some college education because we want new officers to be inquisitive and critical thinkers (although that's sometimes a pain when you are an academy instructor!).

Policing is constantly changing today. There are new threats, new modalities of crime, changing legal requirements, and emerging technologies. The evolving notion of "homeland security" is continually changing the "what's" and "how's" of policing, even if those changes are subtle and incremental. Our officers have to enter this agency with the willingness and capacity to be life-long learners. Policing Youngsville in 2015 is somewhat different from what I did when I first hit the streets in 2005; likewise, how I teach recruits to do the job is different from how I was taught to do the job. These facts are neither good nor bad, they are simply the new reality.

There are other subtle differences between the recruits we see today and the officers I trained with in 2005. I suppose every generation sees differences between themselves and both their predecessors and successors. Most of my academy peers could not remember life without cable television and home computers. Most of the recruits I see today have no conception of life without satellite television, wireless communication, and high-speed, ubiquitous Internet. They grew up playing incredibly realistic video games that did a masterful job simulating reality and conditioning them to receive and process information in order to make quick decisions. A decade ago, most of these games were still very different from the "real world." They were two-dimensional and the graphics were good, but not true to life. Although today's gaming technology is not perfect, it's light years beyond what we saw even a decade ago.

I remember one of my training officers telling me about the old deadly force training simulators they used back in the 1970s and 1980s. Trainees stood in front of a screen where medium-quality, two-dimensional video images were projected. There were a few dozen scenarios, each with a handful of variations. Trainees were supposed to "talk" with citizens as if they were really on the street. The operator could adjust the scenario at one or two points based on how the trainee was handling the situation. The whole focus was on developing the ability to verbally de-escalate situations, but to also recognize when de-escalation was not possible and to understand when deadly force was needed. It was a great technology at the time and was better than anything else that had been developed, but it was also about as realistic as a wooden nickel.

Although YPD does not have the money to afford the cutting-edge training simulators developed for policing, there are some incredible

products on the market. At a recent trade show I was able to test out one of these “sims.” The computer-generated audio and video are incredibly realistic; you know it’s not real, but you have to keep reminding yourself of that fact. Officers can interact with the characters in the sim; this interaction is instantaneous and infinite. With the old simulator, most rookies knew the scenarios and their variations before they ever stood in front of the machine; the possible outcomes of a situation were very limited. These new sims are not just focused on deadly force decision making. They can train officers to deal with domestics, a wide variety of traffic stop situations, questioning witnesses, and virtually any activity a cop might have to perform. Although we could do these scenarios with instructors or actors, in the long run it’s cheaper to have the sim. Also, because the environment is computer generated, the overall effect is an experience that is far more realistic than what can be achieved with trainer/actors operating in a mock apartment on “Hogan’s Alley.” The sims are also more accurate at remembering past performance. A recruit who has had trouble properly questioning victims of crime will be placed in more situations requiring proficiency in that area. If we don’t see improvement, that recruit may not graduate.

The sim technology is going to make training more flexible, both for new recruits and for seasoned officers. In the past, new officers were grouped into medium sized groups who went through their pre-service training together. People who had trouble in a given area (driving, firearms proficiency, report writing, etc.) might get a little extra attention, but everyone pretty much went through at the same pace. In a few more years, that won’t have to be the case. A properly equipped training facility could train a handful of recruits as needed. Although various legal issues and mandates will restrict customizing the training process,

recruits who exhibit more proficiency in areas could be accelerated through the program. Recruits who have problems can get more customized remedial training to help them meet established standards.

At the beginning of every academy class, each student is assessed to determine what learning modality will serve them best. The bulk of the students still elect the traditional route to learning, with lecture being the main method of delivery (reflecting the impact of their secondary and collegiate educational experiences). A small number have alternative learning or testing methods incorporated into their learning plans, which has sharply reduced (though not eliminated) the need for “remedial” instruction later in the process.

However, even with the old standard lecture-presentation format, the classroom looks much different. These classrooms are ‘smart’ beyond what we had in 2005. Each student has a department-issued Personal Digital Assistant (PDA) to access a host of training resources and a vast library of materials written about all aspects of policing. They can use their PDA to take notes, work on assignments, follow along in an instructor’s lesson, and access tutorials. The PDAs are not connected to the main department network, so students cannot access the secure databases available to officers in the field. They can, however, access “dummy” databases to learn how to run checks, conduct data queries, use various YPD databases and online report filing systems, and conduct basic crime analysis.

In 2007, on my second anniversary, I met with my department mentor and revised my Individual Professional Plan. (IPP). Since I was finally sure that law enforcement was what I wanted to do, Cpl. Appleton suggested I think about completing my bachelor’s degree and submit my Professional Request for Training (PRT) for the next 2 years to the training and development sergeant.

Shortly after that, I began an online program to complete my bachelor's degree. My timing was perfect, since I completed my degree and was promoted to corporal right after my fourth year of duty.

In 2009, my revised IPP included my desire to continue with my formal education and attain my master's degree. Soon after I began my coursework at a local university, I got married and bought a house, so I had to shelve my formal education for a while. My life got a lot more complicated in late 2010 when I gave birth to twins. I was able to work up to until my 35th week in a light duty position. I took three months off to be with my babies and then was able to return to work on a 60-60-job share with another new mom. I didn't realize how lucky I was to have that option. My friends at other departments had to make the hard decision to go back to work full-time with infants at home or quit the job they love. I was able to take advantage of the department subsidized childcare at a site close to my assignment. After job sharing for a year, I returned to full duty in 2011.

At my bi-annual meeting with my mentor in 2011, my personal and professional goals were really taking form. I slowly began to take courses towards my master's degree and I requested advanced training in the areas of community policing, homeland security, instructional effectiveness and supervisory leadership. In 2013, I completed my master's degree through an online program and was also promoted to the rank of sergeant.

Some essential qualifications to attain the rank of sergeant have remained pretty much the same since I joined the force in 2005. I was required to have a four-year degree in any field and five years of experience as a police officer. I had to receive consistently favorable employee performance evaluations. I had to demonstrate a commitment for professional self-development and

a record of continued training. Just like officers now, I had to show an ability to work under general supervision and instruction according to established law enforcement practices and YPD policies, procedures, and rules. I worked independently, as well as maintained effective working relationships with co-workers. In 2015, we all must still show an ability to maintain a proper degree of stress tolerance, including stability of performance under pressure and opposition. And of course, I accepted shift work that required working nights, holidays and weekends. This will never change in our line of work, especially in Youngsville.

Sergeants are expected to analyze work unit needs and allocate resources accordingly. They develop work schedules and make personnel assignments. Before I was promoted, I completed voluntary academy training in the areas of management and leadership. In these courses, I had to learn how to review staffing deployment to ensure an efficient and effective utilization of resources. My Sergeant in 2007 helped mentor me when I told her that someday I wanted to be a Sergeant. She taught me how to provide direct guidance on field or administrative matters, and how to conduct staff briefings with peers and subordinates. She also allowed me to observe her demonstrating these skill sets.

My sergeant and my department mentor taught me how to formulate work unit goals and objectives, to set goals and objectives for employees and to follow up on the attainment of these goals and objectives. Whether 2005 or 2015, a Sergeant has to meet with subordinates to identify ways to improve work unit effectiveness and evaluate employee job performance, both orally and in writing. I still meet with other supervisors and staff to resolve problems, participate in information collection for budgeting, purposes, perform research, and serve on committees. Sergeants now as in 2005 establish

and maintain constant lines of communications with internal and external elements of the department; complete special projects, assignments and investigations and keep management apprised as to matters of significance.

There have, however, been changes in how sergeants perform their duties. I have to evaluate reports, overtime slips, leave requests, and other documents submitted by subordinates for accuracy and completeness. I have to update employee logs, writes memos, letters, reports, and employee performance appraisals, as required. I still brief subordinates on new or revised policies, procedures, and rules, clarify directives and standards of performance, and communicate subordinates' concerns through the chain of command. I inspect subordinates' performance, grooming, appearance, and equipment, as necessary. In 2005 this required much typing and keyboard work, now in 2015, the YPD has voice activated software and forms seemingly complete themselves. That still hasn't done away with keeping track of everyone's performance and personal meetings to give appraisals, but it has changed how we handle these matters.

One of the most important duties of a Sergeant is to maintain close contact with individuals in other law enforcement agencies and other public and private entities and to participate in community/public-relations activities. As when I started, at YPD a Sergeant is expected to attend public meetings and discuss problems and provide responses to community leaders. This has become increasingly important in the past 15 years as terrorist attacks increased. It is important to respond to news media requests for information and write news releases that apprise citizens of crime and terrorist activity. Citizens have given up much privacy in the last 15 years to combat terrorism and computer identity theft and it is imperative

that Sergeants respond to complaints and service requests from citizens and political leaders and serve as liaison to various elements of the community and government.

When I was a rookie cop in 2005, sergeants had to identify personnel training needs, conduct in-service training for incumbents and new employees, prepare and present lesson plans and related materials as necessary. I still have to evaluate training received by subordinates and review and submit training records and reports, all while participating in in-service training programs as a student to stay current as mandated by my state. It has always been important for sergeants to coordinate work with other unit supervisors, as well as public and private entities, but this was nothing compared with modern demands. Now, many non-law enforcement, technical, investigative, and administrative functions are privatized and out-sourced while traditional duties and responsibilities are handled by YPD. In 2005, private security began to take on responsibilities such as guarding prisoners who have been hospitalized and the protection of major crime scenes including homicides. By the time I became a sergeant in 2012, the YPD had formed a variety of partnerships with both public and private entities due to lack of personnel, knowledge and resources with which to combat cyber crime, manage diversity, and provide up-to-date forensic investigation.

For example, crime scene investigation advanced between 2005 and 2015. The sequencing of the human genome has increased information obtainable from a DNA sample. Characteristics such as eye or hair color or age may be obtained to form a description of the suspect. A DNA computer became available in 2010 but the cost is high and expertise is limited to specialists so a few companies provide this service to many departments. Chemical cameras that link electronic

with biological systems take pictures and detect other elements such as blood or use luminescence to identify crime stains. Augmented reality video, audio and sensing devices, and medical imaging devices have enhanced forensic data available at the scene. Again, this equipment is too expensive to be purchased by one department. Mutual Agreements of Understanding have been formulated. In 2015, nanotechnology has made diagnostic and analytical equipment cheaper but it is still expensive and not yet disposable. This increasingly dynamic environment has led to the development of a private business industry based on the collection and analysis of forensic evidence. In some jurisdictions, these private entities are contracted to provide crime scene services, particularly where agencies cannot afford the expense of acquiring requisite equipment and training personnel on its use. Similar private business ventures have emerged to meet the growing needs in cybercrime investigation.

In the last ten years we have also seen changes in how agencies train officers for promotion and advancement. I was lucky enough to attend Enlightened Leadership Training in 2007. The YPD was committed to changing the culture of the department. This training helped create an environment that expedited the natural maturation process that all people must go through to allow their inherent leadership abilities to emerge. It also developed a truly shared, inspiring process vision for guiding the way through times of uncertainty. This process has served all personnel well during the last 10 years, when more was expected with fewer resources. I learned to ask personnel the right questions—effective questions. These questions are powerful tools for bringing out the best in people. They break down resistance to change and let people openly communicate and take personal responsibility. They helped promote leadership in a

team environment.

Questions can devastate us or they can empower us. We stopped asking questions such as “What’s the problem here?” and changed the question to “What aspects of this project are you most pleased with?” This type of question has encouraged my personnel to take more responsibility and I think it helps develop leaders. I also ask my people what ideas they have to help us move forward in the YPD. These effective questions have helped bring out the best in my staff since my promotion in 2009.

Training itself is somewhat more convenient now. By 2010, the YPD provided classroom training on the Internet. Now in 2015 virtual and Augmented Reality training programs are provided regularly by a private company dedicated to training law enforcement personnel. Standardized education among agencies was necessary due to the continuation of terrorist plots and attacks in the U.S. These programs allow the simulation of dangerous situations in controlled settings and provide proven ways to combat situations that in 2005 were rare but today are common.

Before I became a police officer in 2005, there was a real wake-up call. September 11, 2001 brought terrorism to the doorstep of America. It propelled me to a career in law enforcement. The YPD, like every law enforcement agency in 2015, is playing a part in homeland security. After many turf battles, communication networks linking all law enforcement agencies became a reality in 2010. Since 2005, terrorism has taken many forms such as attacks against the infrastructure through our computer networks, weapons of mass destruction (nuclear and biological), genomic or genetic terrorism attacking food production and preparation, and traditional random violent attacks. The National Intelligence Council predicted that terrorists’ attacks would become more sophisticated and achieve mass

casualties by 2015 and they were right. The attacks on the Minneapolis Mall and the shooting down of five airliners with shoulder held missile launchers were horrendous. A small group of terrorists were responsible for these actions. The discovery of a nuclear device by LAPD personnel was also eye opening. Without violating the constitutional rights and guarantees of our citizens, we have had to develop practices and policies that address all forms of terrorism.

Between 2005 and now, job descriptions have had to be continually revised to reflect the changes in technology and changing events. Sergeants and other officers have to be able to communicate with the private sector employees who handle tasks formally assigned to sworn officers. Recruitment plans had to be developed to ensure a diversified workforce; greater value is now placed on more highly educated officers with backgrounds in technology, strong communication skills, fluency in more than one language, and an understanding of various cultures and current events. Minority populations have increased dramatically. They predicted that by 2020 more than 38% of the United States population would be minorities and I would say that in 2015 we are nearly there.

In 2010 biometrics were used as an identification tool in everyday life such as in bank transactions and facial, voiceprint or retina recognition devices for identification of criminals. The national ID cards that became law in 2006 have been replaced by biometric scanning, requiring a whole new training program for all personnel...and to be coordinated by the Sergeants. I helped develop these classes, and they continually need to be updated because of changes in technology.

Nanotechnology, developed in the early 2000s, allows the manipulation of matter and enables the storage of enormous amounts of data on the size of a button. Wireless and nanotechnology

allowed advance wearable computers to be developed, providing instantaneous information about an officer's current environment and location, immediate language translation, and information about crimes and criminals in the area of patrol. The devices facilitate on-the-spot interfaces with biometric recognition databanks, allowing officers to identify wanted individuals immediately, merely by observing people on the street.

Super lightweight armor that provides ballistic protection has been developed. Non-lethal options for subduing violent criminals are now commonplace. Sensors have been designed to notify officers of biological, chemical or explosive contamination and technologies allow officers to detect concealed weapons on suspects. Using energy stored in their shoes, police officers can easily climb over 10-foot walls.

But most importantly, the increased use of robots has removed much risk to officers. I can send the gnatbots in to survey a scene where a suspect or terrorist is holed up. They're so tiny they are rarely detected as they scoot under the door or through cracks in windows. They can deliver pictures and confirm the identity of the person using biometrics.

Change has been rapid in the last 10 years during my career. Good management and leadership transcend time. The biggest challenge has been keeping staff trained on the ever-emerging technologies, meeting the challenges of terrorist attacks and communicating effectively with the public. In 2015 and beyond new police recruits will be cross-trained. I will need to know more about fire-fighting and emergency services. Due to budget restraints, this cross training has become necessary because cities are demanding that police departments become public safety agencies that incorporate all these functions. Youngsville is currently studying this concept. White-collar crime and identity theft have been a problem since 2005. In

order to coordinate and communicate with our out-source providers, I will be required to know much more about the investigation of complex computer crimes and more importantly about crimes against the older citizens of the community. As the use of the Internet has increased by all members of the planet, so have demands on my skill level.

Seniority has become a dead issue and promotion will be based more upon my social skills and community involvement. I must improve my skills concerning teleconferencing since roll calls have been eliminated and officers in their homes can retrieve information before their watch begins. Cameras are everywhere in Youngsville and the U.S. and I now have to know about closed circuit television and how it functions. We have schematic drawings that show the interior of all businesses, schools, and warehouses in Youngsville.

I will, on occasion, act for the captain during her absences and execute general and special assignments in the planning, administration, coordination, direction and review of the division operation. I will identify personnel training needs, coordinate training activities, and participate in training programs as an instructor. I will provide direct supervision, guidance and training to police sergeants and may supervise civilian personnel. I will be called upon to mentor and coach subordinates as required.

Management styles have changed, with the emphasis being placed on leadership ability and interpersonal relationship building. Special training and career development opportunities are required to retain employees as well as to maintain professionalism. Teamwork is the norm and the old military style hierarchy has been replaced with situationally defined team-and network-based protocols (while some of that is now almost second-nature to the senior officers, it requires a constant training presence—a “guiding hand” in supervision,

if you will). Organizations now place emphasis on professional values instead of bureaucratic control of employees, but recruits coming to us from service-sector and manufacturing backgrounds bring command-and-control expectations that are sometimes hard to “un-learn.” In 2015, the Youngsville Police Department must deliver policing services with identifiable performance measures and clearly state the vision, the mission and values statements that will be implemented by the department.

It will be my responsibility at times to represent the YPD and the city in front of various civic, professional and special interest groups. I will participate in community and public relations activities, attend public meetings, and discuss problems and responses with community leaders. Citizen involvement has increased and is paramount. Community policing has incorporated process mapping to a higher degree. Satellite transmission of GPS data and mobile computers in police cars and worn by individuals are the norm. Tracking trends in crime and neighborhood demographics gives officers in the field instantaneous information. The move toward urbanization has increased access to information and other technological advances. Citizens are able to log on and track crime in their neighborhoods and vote on issues affecting them. Their homes are ‘Smart’ and notify YPD of intrusions.

I recall a quote by Alvin Toffler given to me at a Police Futurist Class in 2010, “An acceleration of change has consequences that are not necessarily a result of whether the change is good or bad, but just acceleration in itself creates consequences and some difficulties for us.” I have been in law enforcement for 15 years during which time the world and law enforcement agencies have changed dramatically. Some of these changes were foreseen, some not. The same will hold true for the next 15

years and I am confident the police officers of the future will meet the challenge.

Goals for the Future of Training

There is considerable distance between the current state of police training and the world of Sgt. Melina Grace. A number of the elements are already maturing, though they are more exemplary than industry standards, for the most part. Training, like education, is still very much based on a “sage-on-a-stage” model of didactic lecture, delivered in a standard format to a massed audience.

One goal for training in the future is for it to be flexible, adaptable, and on-demand. With the advent of Web-based learning, a considerable proportion of the content that is currently delivered via classroom lecture no longer requires a classroom. New recruits can be required to study and learn statutes, case law, and a sundry other topics on-line before they report to the Academy. The first several days would consist of familiar testing to gauge the assimilation of those background, “factoid” materials. Thenceforth, academy learning would proceed on a scenario-based premise, applying the basic knowledge to tabletop, role-playing, and virtual scenarios.

In-service training will also be enhanced. At the present time, the limited number of compulsory hours tends to be devoted to instructing officers in changes in statutory law, the implications of new case law, and occasionally some skills-renewal exercises. Once police organizations are better linked to the online world—interacting online instead of watching videos (essentially “lectures on tape”)— in-service training can take a much different form. Basic information dissemination will be done in timely fashion in roll call (as it is done in many agencies already); “training” will be spread out over time, with scenarios mimicking the real-time development of problems. Instead

of being absent from duty for an entire week, bored to tears in a classroom (or asleep at the back of the classroom), training will take place in modular segments, interwoven with shift work (as the situations might well be in real life). “Come together” time can be limited to initial briefings (if needed) and the more important post-action assessment.

The technology Sgt. Grace appreciated will be available—indeed, prototypes and some early production models already exist, but are not widely available. As other authors in the volume note, the technology will develop much faster than local or even state budgets grow the capacity to purchase and deploy it in standard issue. Much of the high-end technology will just not be affordable in all areas. The slack can be taken up, as it is now in special-skills and trans-jurisdictional needs, through collaborative purchasing. On-line training sessions will help raise the bar for all officers to become familiar with the new technologies, not just the fair-haired few who were fortunate, senior, or favoured enough to be sent to a special off-site school. While not every officer will be sufficiently trained to be assigned a technology-specific role (as the tragic death of Victoria Snelgrove in Boston recently demonstrated), most officers will be sufficiently familiar with the capacity of the various technologies to be able to participate in team responses where the technology is critical.

Unless we anticipate (as some of the scenarios in this volume do) a radical and fundamental change in the nature of American policing in reaction to a wave of successful terrorist attacks, changes in training and education will be evolutionary. (In a war-based scenario such as Melis and Myers outline, police training likely would be far more militaristic than anything outlined here, for instance. Trying to conjure up a training vision for such an eventuality nudges us toward the realm

of fiction rather than futures.) The groundwork for evolutionary change has already been laid, and we can anticipate a greater emphasis on training as life-long learning. As management practices mature, and adapt to the new demands of homeland security, lateral and virtual communities, a much more vibrant multiculturalism, and the like, recruitment will perforce change. Advanced training such as we envision depends upon the adaptability of youth, and broader vision of service than “cuff ‘em and stuff ‘em” law enforcement. The same technologies that enhance training can be adapted to improve efforts to recruit actively, and to select individuals suited to the new demands of policing. Once hired, the adaptable, on-demand training capacities can also prepare individuals for supervisory roles. Promotion need not be based solely upon seniority (or a test score, or creditable service records in the job to be left), with a hold-our-breath hope that they will be able to handle their new responsibilities. Candidates for supervisor and managerial positions, and specialty functions at the line level, can be identified in advance, encouraged, and prepared for their role through a variety of formats. All personnel, regardless of rank, experience, or career trajectory, will amass a portfolio based in part upon training and testing, giving management the broadest possible insight into candidates’ strengths, weaknesses, and potential.

All of these capacities are present, or on the near horizon as this is written in 2005. More will be available, often from unanticipated sources, as we move toward the year 2015. The challenge for the near future is nevertheless much the same as it has always been: to be aware of the changes in our environment, to actively seek out ways to improve, to capitalize upon the improvements of others, and to constantly strive to make ourselves better with

whatever means are at our disposal.

Endnotes:

¹ Robert Gallati, “Some Modern Horizons in Police Training,” *FBI Law Enforcement Bulletin*, September 1957, 7.

² Michael E. Buerger (1998). “Police training as a Pentecost: Using tools singularly ill-suited to the purpose of reform,” *Police Quarterly*, 1, 27-63.

³ California Assembly Concurrent Resolution 58 Study Committee Report to the Legislature, *A Vision of Excellence; California Law Enforcement Training in the 1990s* (January 1991): 15.

⁴ ACR 58: 16.

⁵ George Korzeniewski, “Survival City”, *Law and Order*, October 1990, 31.

⁶ David L. Carter, Allen D. Sapp, & Darrel W. Stephens (1989). *The State of Police Education: Policy Direction for the 21st Century*. Washington, DC: Police Executive Research Forum.

⁷ Buerger (1998).

⁸ Matthew J. Hickman (2004). *State and Local Law Enforcement Training Academies*, 2002. Washington, DC: Bureau of Justice Statistics.

⁹ Ironically, the formal processes aimed at helping trainers learn to teach often exceed the formal processes used to ensure those in higher education have the skills to teach.

¹⁰ Hickman (2004).

¹¹ See Gene E. Carte and Elaine H. Carte (1975). *Police Reform In the United States: The Era Of August Vollmer, 1905-1932*. Berkeley, CA: University of California Press. National Advisory Commission on Criminal Justice Standards and Goals (1973). *Police*. Washington, DC: U.S. Government Printing Office. National Commission on Law Observance and Enforcement (Wickersham Commission) (1931). *Report On The Police*. Washington, DC: U.S. Government Printing Office. President’s Commission on Law Enforcement and the Administration of Justice (1967). *Task Force Report: The Police*. Washington, DC: U.S. Government Printing Office.

¹² <<http://www.interlog.com/~blake/nov99/toffler.html>>

Privacy 2015

Michael E. Buerger

Few of our fundamental concepts are under greater pressure than that of privacy. It is challenged overtly in the name of national security by the provisions of the USA Patriot Act, and covertly by the unexplained and unexamined small print of commerce. It is challenged not only by technical engineering, but also by the social engineering that has arisen from enhanced technological capacities. The questions of whether privacy as we currently understand it will still exist in 2015 seems to lie in the balance in 2005.

In American law, legal concepts of privacy derive not from explicit articulation, but from “penumbras” of other principles and words within the Constitution and the Bill of Rights. Those documents were written in an era when the world of physical space constituted the entire known universe. When the Fourteenth Amendment was written, long-distance communications were the province of Samuel Morse’s telegraph, and age-old technologies of drumbeats, smoke, and physical transportation of written messages. The modern emergence of cyberspace has created a virtual new world in which space and time are compressed, altering the fundamental rules by which we have lived. Chief among those changes, cyberspace has bestowed upon almost all of us a parallel identity that is virtually limitless, disconnected from our physical “real” selves, and in important ways not under our control.

It is not so much that cyberspace created new problems, because the privacy and identity problems that plague us today have analogs in the physical world. Rather, the speed and scale of information transmission in the Information Age exacerbates those problems, substantively transforming them, magnifying their power, and perhaps creating

something fundamentally different from their historical cousins.

Our notions of privacy are anchored in the concrete, physical world of agrarian England, ghosts of a world long gone. Thomas Cowper (in this volume) rightly speaks of our understanding of information as an artifact of the Industrial Age, but the accelerated change of technology is asynchronous with the social developments that use, constrain, retard, or banish technology. The modern age is a battleground in that sense, between shifting alliances of forces that alternately embrace or renounce technological advances according to principles and desires that are disconnected from the technology itself. The challenge presented by the onslaught of technology is whether it will be a master or a tool; the current interrelated debates over the extent of privacy similarly inquire whether a concept so anciently conceived can long endure.

Personal, Private, and Public

Whether “a reasonable expectation of privacy” survives to 2015 in any form depends upon the arc of developments in three main areas:

- 1) the personal decisions of individuals to surrender their expectations of privacy voluntarily, or haphazardly, in search of some thing or things deemed valuable to them;
- 2) government restrictions placed upon private sector use of data in the interests of a recognized “common good”; and
- 3) legal restrictions upon government’s use of data and technology.

It is possible that “a reasonable expectation of privacy” is a frog, slowly being boiled without understanding what is happening to it. As technological advances becomes so pervasive, and the economy so dependent upon credit, the law

finally may bow to the commonplace reality and no longer require obeisance to an archaic 18th century notion. The alternative possibility is that real and perceived abuses will mobilize the citizenry to take steps to reassert the centrality of “the right to be left alone,” not only by the forces of government, but also by the titans of industry and finance.

A central question in the debate will be whether my individual control over the multiple ethereal abstract renditions of “myself” that exists in the databases constitutes a fundamental right. If it is, a host of regulatory actions may be taken by government. If it is not, we enter into a brave new world with fundamentally different expectations of the nature of society and social interaction.

Expectations and Limits

Advocates of greater information-seeking tools consistently remind us that privacy is not synonymous with anonymity, and that anonymity is neither a right nor a reasonable expectation. That remains true, but was also true in the physically defined world. None of us are invisible, able to pass through public space without being observed. Few of us maintain solitary lives “off the grid,” though many live with relative anonymity in the turbulent flow of humanity in the cities.

Physical protections of privacy could be overcome—conversations could be overheard; non-verbal actions, reactions, and signals observed; written communications read over the shoulder—but with some balance. Physical proximity was required to eavesdrop, and with proximity came the counter-threat of exposure, alerting the target to the surveillance, and allowing countermeasures (including silence, deferring communication to another time and place, the use of codes, etc.). As communications expanded over longer distances by telegraph, telephone, and radio transmitter, more

surreptitious interceptions became possible. Security depended upon codes, and luck. (The use of the Navajo language by the Code Talkers in World War II stands out as a prime example of successful code protection, but it rested upon the physical and social isolation of the Navajo Nation from the Japanese. Whether a similar scheme could be as successful today is perhaps more problematic).

Several things have changed in the balance with our newest technologies, but three stand out. First is the permanence of the information—or, perhaps viewed from a different perspective, “the abstract representation of the individual, bound in time”—obtained, and its imperviousness to outside challenge. Second is the ability of the information-seeker to acquire and use the information in stealth. The third and perhaps most important area of concern is the susceptibility of the information to be used or altered without the knowledge of the individual it represents. A fourth problematic change looms in the background: the possibility that those who use the technology to seek exposure rather than privacy—the bloggers and exhibitionists—will somehow alter the terms of the debate, to the point where social expectations are of transparency rather than privacy.

(1) Permanence and Imperviousness

Our embarrassing and inglorious moments have always been observable to others (indeed, that visibility is usually the source of the embarrassment). In the physical world, they are largely confined to memory, and recede over time in both clarity and importance. While our temporary loss of dignity could be shared with others, it was largely a pale version, relayed verbally (with or without embellishments, to be sure), and a moment in time. The retelling could even work to our benefit, if the teller of tales was regarded as a gossip: distortion might be presumed by the audience,

diminishing the credibility of the report regardless of its accuracy. The observation that “your friends will know what’s true and your enemies will assume what they want” could operate with relative ease. Even in cases where our lapses were known to be true, they constituted but one moment in our long association with friends and neighbors. Visual representation changes that dynamic, whether captured by closed-circuit surveillance cameras, a voyeur’s hidden camera, or cell phone cameras of friends and associates.

Non-visual representations of self have been likewise transformed. If I had trouble paying my bills at one point in my life, in the immediate world my friends, associates, and neighbors know and remember it, but are also aware of my more recent history of fiscal responsibility. Their judgments of whether I am worthy of their trust will be based upon the totality of circumstances, presumably with the more recent given greater weight on the basis that they are more representative of my current abilities and disposition. In the new world of cyberspace, there exists no grace period in which to correct errors, no chance of recovery, and no redemption: our ghostly selves may drag Marley’s chains with them forever.

Proponents of the wider use of technology point to a small group of incidents in which the unflinching eye of surveillance cameras helped resolve a case. From the Bulger case in London to the abduction of Carlie Brucia in Florida, televised images have aided in the solving of crimes. Opponents point to the less certain impact of CCTV on crime prevention, and to the early failures of biometric scanning at public events (Reuters 2003). They question not only the difference between the social cultures of the United Kingdom (where CCTV is widely used and widely accepted) and the United States (where CCTV in public spaces is still a relatively rare phenomenon, and less widely

acclaimed), but the deterrent effect itself, citing numerous individuals who rob convenience stores and banks, despite the obvious presence of security cameras. The Beltway “cell phone bandit” is but the latest and most intriguing of a long line of rieviers who are either oblivious to or contemptuous of the technology set up to deter or ensnare them.

(2) Stealth Acquisition

In one respect, “privacy” is less the issue than security. In order to participate in modern life, we have little choice but to part with a certain amount of information about ourselves. To obtain credit, we must demonstrate that we are worthy of it, that we have a history of paying our debts, that we have assets commensurate with the risk we ask the lender to take with us. To obtain and use health benefits, and insurance, we have to divulge certain information about our habits and conditions so that we may swim in the appropriate part of the actuarial pool. In all of these endeavors, we are supplicants: we ask a larger polity for goods, services, and benefits beyond our individual ability to obtain. Most of us enter into those communal arrangements willingly, and with a tacit belief that the surrender of information is done in confidence, a dyadic relationship between ourselves and the service provider.

Technology altered the ground upon which we stood. When record keeping passed from paper files to electronic databases, the ease with which information could be shared expanded exponentially, and the cost dropped dramatically. In a nearly Orwellian transformation, things that were not forbidden suddenly became things that were permitted. Nothing existed that said personal information could not be shared, and so it was shared. Entire industries sprang up to sell information to other industries for marketing, and for other purposes masquerading as “research.” In

the absence of legislation or regulation requiring that we be contacted when our supposedly confidential information was sought by others, the acquisition of wholesale batches of information became routine, subterranean, and profitable.

Technology also opened the way to another form of stealth acquisition: theft by hacking. The relatively open systems of commerce, with their relatively simple attempts at security, became the sneak thief's playground. The year 2005 brought news of multiple breaches of supposedly secure databases, and the loss or compromise of important information from ChoicePoint, Wells Fargo, the United States Air Force, several universities, and many supposedly protected sources.

(3) Transmogrification: Alteration and Suborning.

When a surreptitious video of public behavior can be easily made and posted to the Internet, that behavior is enshrined to an unintended, perhaps undeserving audience. If the video is edited and transformed into something it is not by compressing two separate actions into a single sequence (the act of picking one's nose, spliced onto the act of eating some popcorn, both occurring at separate times in a sports arena seat, for instance), a visual slander has been created. While the example here is relatively mild (it is an actual event, with crudely obvious splicing, viewed on a colleague's computer some years ago), the potential for greater trespasses is clear. "Seeing is believing" has first claim on a viewer's allegiance; its corollary, "believing is seeing," is often consigned to the dimly lit background.

While there is a question of whether or not we can be "harmed" if such an image is viewed by countless persons we will never meet in real life, nevertheless a fundamental shift has taken place. The amount of exposure to ridicule for everyday actions and conditions—once the sole realm of

public figures and their paparazzi—has been foisted upon those who never sought to be public figures. The level of discomfort is only slightly lessened by relative anonymity: the threat of being accosted in a public setting by a cry of "Omigawd, it's the Booger-Eater!" lurks at the periphery of our vision.

Once upon a time, the closest we came to earthly immortality was to be on a mailing list. Those primitive databases seemed to last forever, oblivious to the passage of time...the inverse of fading human memory. On the Internet, they are not only timeless but replicatable, alterable. The most dramatic depiction of the potential for mayhem is the Sandra Bullock film *The Net*, now somewhat dated and a shade too Hollywood, but still a reasonable demonstration of the potential for mischief. At the core of the movie is the premise that the electronic representation of one's self is far more readily accepted in modern life than the corporeal self: the individual is dependent upon testimonial verification by their electronic *döppelgangers*.

Identity theft is easier than identity replacement, but even simple pranks and dirty tricks can cause mayhem. Hacking into online sex offender registries to delete records would have bad enough consequences. Were a malefactor to hack into one or more to create a false record bearing your information would be catastrophic (the basic premise of *The Net*). There are multiple means by which the slander could be verified as false, but almost all of them would come into play only after you were falsely and publicly branded as a pervert, a terrorist, a fellow traveler. As victims of even the simple financial identity theft have testified, the process of setting matters right again is tedious, lengthy, and painful.

Behind the notion of a "record" lies a need for some permanence of knowledge, a standard against which new information can be tested. Also implied in that permanence is the concept of

importance. From the first development of cylinder seals and cuneiform pictograms on clay tablets, commerce has depended upon records. Notations of births, marriages, and deaths written into family Bibles establish the linear descent of a clan, and the important linkages to others through marriage. The concept of sacred scriptures themselves—words so important they must be preserved forever, to inform exactly each new generation—epitomizes the deeply human need for a vehicle that conveys Truth (and its secular cousin, truth) across time and distance.

From clay tablets to data packets, economic and social stability has rested upon the foundation of a permanent record against which disputes could be tested. As the certainty of the records erodes under conditions of rapid proliferation, unverified augmentation, and potential distortion, there may be collateral losses in several spheres. A decline in consumer confidence may result in a constriction of the economy. To date, we have been concerned primarily with individual identity theft; if a second-stage corporate identity theft wave develops, it could affect capital projects, mergers, and the stability of trade. Unauthorized transfer of assets to offshore accounts, blocking of legitimate transfers to obstruct a purchase or payment, overwriting e-mail records with bogus “evidence” of wrongdoing and other forms of attack all undermine the foundations of legitimate commerce.

Unlike individual identity theft, we can predict that the resources to combat corporate theft will be considerable, and brought to bear in short order. Nevertheless, the impact of one incident will have ripple effects far beyond whatever damage is inflicted. As soon as the first case of corporate e-spying takes place and becomes public knowledge, all corporate systems are both fair game, and suspect. E-spying of the above-described sort may have occurred already, and kept behind the veil of proprietary information. The hacking arts

embrace the ability to part that veil, however, and greater scrutiny of corporate records may result from both the Enron/WorldCom class of scandals and from the data mining brought to bear in the wars against terror and drugs.

The current line of forward thinking on such matters posits that “transparency” is the only reasonable defense against the suborning and misapplication of data. While that yet may be the case in some utopian future, in this particular arena the dictum that “the future is here; it is just not equally distributed” is most acute. Transparency cannot work for the individual unless corporate decision-making is equally transparent, and that is unlikely to happen in the near future. Government transparency is equally unlikely, even if some inroads are made into the present levels of over-classification of information. Secrecy acts against transparency as a form of Gresham’s Law: as long as there are some secrets, there is no transparency, only selective exposure.

(4) Evolving Social Expectations

Beyond the international debate over ICANN and Internet copyrights is a second level of the question, “who controls the Internet?” Those who value privacy are invisible on the ‘Net if they wish to be: until the day that money disappears, and all financial transactions are electronic, “protected” by biometric security measures, use of the Internet and the World Wide Web is voluntary. That may change by 2015, if the future is linear and driven solely by technological engineering, and Internet transactions become compulsory because they are the only game in town (outside the inevitable black markets that would develop). Social engineering remains a powerful force, however, and the disappearance of a cash economy is not a given.

The concurrent debate over illegal immigration and day labor, for instance, exists in

part because payments to migrants are (or can be) made in cash. Similar gray-market arrangements exist in childcare, elder care, automobile repairs and home improvements, among others, because smaller amounts of cash are essentially untraceable. If a combination of homeland security and taxation issues combine to eliminate paper money (which then would finally and literally be “not worth a Continental”) in favor of traceable electronic transfers, we should anticipate a huge social dislocation of labor. The change will affect the undocumented and the non-documenting alike, and will have reverberations probably far beyond those of Sarbanes-Oxley.

The public face of the ‘Net is those who use it for exposure, through blogging and webcasts (and the most recent innovation, podcasting). In a reversal of the “most embarrassing moments” material above, the Internet seems to thrive on them. Television had already staked out the ground, of course—from the old “Queen For A Day” show to the hapless and hopeless on “American Idol” and “The Apprentice”—but the ‘Net widens Amateur Night astronomically. The bizarre celebrity of the Numa Numa dance (Feuer and George, 2005) may temporarily shame the protagonist, but perversely inspires imitators. Blogging does not just give voice to the closet Einsteins and Jeffersons and Hunter Thompsons of the age; it also provides a forum for the wildest opinions of every village idiot and drunken sot who can keep it together long enough to string words together on the keyboard. Indeed, with current estimates of 30% of Web traffic being sex-related, and a considerable underground developing for all sorts of antigovernment types (from the radical right of America’s Christian Identity splinter groups to the democratic forces within China to the postings of al-Qaeda and the Taliban), there is a danger of a Gresham’s Law here, as well. Codes of conduct may not be sufficient to curb the tendency

to the lowest common denominator: outlaws scoff at codes, and only heed them when effective enforcement is imminent.

It is not bad enough to be expected to have a web page; everyone can also be Googled. While that is little more than what was possible with paper-driven systems, the ease and speed of the Internet search engines create an easy exposure that can be exploited by persons who wish us ill. The problem of stalkers using open records to locate their victims has already been widely published; the potential for similar exploitation by kidnappers, terrorists, political assassins remains thankfully unexploited, but a problem nevertheless. A comparable problem for law enforcement officers centers on the availability of their home addresses in online property records files. While many jurisdictions have enacted a patchwork of laws to fill these gaps, their mere existence gives the lie to the notion that protection lies in transparency. At best, transparency provides only limited protection against certain kinds of predations; it creates huge vulnerabilities to others.

This undercuts the premise of those who argue that privacy is dead, and transparency is the only effective defense against the misuse of data. The problem lies in the fact that transparency is like pregnancy—the system cannot be just partly transparent. Neither can one be constantly vigilant, at least not against attacks that can originate in any area of the globe. Part of civilization rests upon the ability to depend upon the integrity of the systems that society builds... and in this respect, the Internet and related technologies (especially the emerging area of nanotechnology and micromanufacturing) remain suspect.

At the Door of the Humblest Hut...

Citizens of the Agrarian and Industrial ages have more in common with each other than either with the emerging 'Netizenship of the Information Age. The physical properties that defined and limited public and private life prior to 1984 no longer constrain the new electronic age, and we are faced with evolving definitions of not only citizenship and economic participation, but of personhood.

The western understanding of privacy stems from the dictum of English Common law that (roughly paraphrased) "at the door of the humblest hut of the lowliest peasant, the King himself must stop and ask permission to enter." It was not the case that the King lacked the physical power to cross the barrier; nor is there overwhelming evidence that the King and his minions often bothered to stop or knock. Rather, the expression embodies a normative expectation that the King *would* do so.

Normative expectations are the product of social engineering, and the idea of privacy established that there was some physical space beyond the control of even Blackstone's observation "That the king can do no wrong is a necessary and fundamental principle of the English constitution." It evolved during a time when kingships aspired to absolutism in Europe, and it endured through contests between church and state, revolution and civil war, and the transformation of the economy from mercantilism to capitalism. The concept of privacy bestowed upon all persons, regardless of rank, station, or lot in life, some small degree of autonomy in the face of the overwhelming political forces of the day.

It was, of course, an extremely limited autonomy. The peasant who refused the King's request to enter paid a price, either immediately or as soon as he left the paltry safety of his humble

hut. Nevertheless, that harsh truth is secondary to the importance of the symbolism: the humblest peasant possessed some quality, some right, to make even the juggernaut of royal prerogative pause in its course. And while it was doubtless honored more in the breach than the observance for much of its history, its normative power grew with time.

The delegates to the Constitutional Convention, with fresh memories of writs of assistance, Courts of Star Chamber, and the quartering of troops in private homes, wrote restrictions upon intrusive government actions into the foundation of this country's government. At the same time, Adam Smith's *The Wealth of Nations* articulated a larger transformation based in the notion of property (physical goods and chattels, including human slaves). Our jurisprudence contains numerous cases in which property itself stands against the power of the State, from the notorious Dred Scott case to the constellation of "United States versus Piles of Money" cases that paint a pointillist portrait of the drug war.

Until the 1960s, privacy vested primarily in the Fourth Amendment guarantee against unreasonable searches and seizures, which implicitly involve the physical world: persons, houses (places), papers, and effects. Social, medical, and technological advances coalesced in a variety of conflicts in that turbulent decade, and the notion of privacy also evolved (at least at law). The Supreme Court decision in Roe v. Wade provided a thumbnail sketch of those developments:

The Constitution does not explicitly mention any right of privacy. In a line of decisions, however, going back perhaps as far as Union Pacific R. Co. v. Botsford, 141 U.S. 250, 251 (1891), the Court has recognized that a right of personal privacy, or a guarantee of certain areas or zones of privacy, does exist

under the Constitution. In varying contexts, the Court or individual Justices have, indeed, found at least the roots of that right in the First Amendment, Stanley v. Georgia, 394 U.S. 557, 564 (1969); in the Fourth and Fifth Amendments, Terry v. Ohio, 392 U.S. 1, 8 -9 (1968), Katz v. United States, 389 U.S. 347, 350 (1967), Boyd v. United States, 116 U.S. 616 (1886), see Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting); in the penumbras of the Bill of Rights, Griswold v. Connecticut, 381 U.S., at 484-485; in the Ninth Amendment, *id.*, at 486 (Goldberg, J., concurring); or in the concept of liberty guaranteed by the first section of the Fourteenth Amendment, see Meyer v. Nebraska, 262 U.S. 390, 399 (1923). These decisions make it clear that only personal rights that can be deemed “fundamental” or “implicit in the concept of ordered liberty,” Palko v. Connecticut, 302 U.S. 319, 325 (1937), are included in this guarantee of personal privacy. They also make it clear that the right has some extension to activities relating to marriage, Loving v. Virginia, 388 U.S. 1, 12 (1967); procreation, Skinner v. Oklahoma, 316 U.S. 535, 541 -542 (1942); contraception, Eisenstadt v. Baird, 405 U.S., at 453 -454; *id.*, at 460, 463-465 [410 U.S. 113, 153] (WHITE, J., concurring in result); family relationships, Prince v. Massachusetts, 321 U.S. 158, 166 (1944); and child rearing and education, Pierce v. Society of Sisters, 268 U.S. 510, 535 (1925), Meyer v. Nebraska, *supra*. (Section VIII)

“Privacy” expanded to include decisions, and while those decision had physical consequences (interracial marriage in Loving v. Virginia; the sale, purchase, and use of contraceptives in Griswold;

abortion in Roe, etc.) it also began to extend to information. The case of Eisenstadt v. Baird is perhaps more salient than even Roe, dealing as it does with the dissemination of information that *implied* actions contrary to a state law. More recently, in Kyllo v. U.S., the Supreme Court robustly defended the Fourth Amendment concept of physical privacy even against “stand-off” technology:

We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area, Silverman, 365 U.S., at 512, constitutes a search—at least where (as here) the technology in question is not in general public use. This assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted. On the basis of this criterion, the information obtained by the thermal imager in this case was the product of a search... At the very core of the Fourth Amendment stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion. Silverman v. United States, 365 U.S. 505, 511 (1961). With few exceptions, the question whether a warrantless search of a home is reasonable and hence constitutional must be answered no.

Writing for the Court, Justice Scalia noted:

It would be foolish to contend that the degree of privacy secured to citizens when the Fourth Amendment has been entirely unaffected by the advance of technology. For example, as the cases discussed above make clear, the technology enabling human flight

has exposed to public view (and hence, we have said, to official observation) uncovered portions of the house and its curtilage that once were private. See Ciraolo, supra, at 215. The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy... We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area, Silverman, 365 U.S., at 512, constitutes a search—at least where (as here) the technology in question is not in general public use. This assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.

At the root of all arguments, Roe established the principle of “personal rights that can be deemed ‘fundamental’ or ‘implicit in the concept of ordered liberty’ ” were protected. While Kyllo anchored the concept of privacy in the 1780s (the cusp of the transformation from the agrarian age to the industrial), it also left the issue open by adding the proviso “at least where...the technology in question is not in general public use.”

It is possible to envision a scenario in which Kyllo is swept aside. Adapting the technology to an on-street fire detection system, passively monitoring building heat via sensors on utility poles, would be a potential way to detect sudden changes in heat levels that suggest the early start of a fire. Such a system could augment or replace existing smoke- and fire-alarm systems, or provide a public alarm source in areas where privately maintained systems are unlikely. A street-mounted system would have an advantage at night, when occupants are asleep, and during periods when the occupants are away. In

multi-family dwellings, fires that erupt in unattended common areas would be detected. And so, too, would any unshielded hydroponic marijuana farms and other drug-production facilities using high heat.

Technology has fundamentally altered our perceptions of physical space. The Kyllo opinion also recapitulates an observation from the Dow Chemical case, noting that routine aerial flights created a different perspective of lands, a “third dimension” of surveillance that was once restricted to a two-dimensional plane (the Court in Dow made a distinction between commercial properties and 4th Amendment-protected private residences). To those routine airline overflights we must now add satellite photography and mapping, mini-cameras and radio-controlled model planes, both of which neutralize the ground-level fence as a defense of privacy. Widespread ownership of digital camcorders, cell phone cameras, telescopes, and the like all erode the expectation that our actions will not be recorded, and our ability to limit such intrusions. A similar argument is being made for the data-mining industry, which enjoys seemingly unrestricted access to information compiled from multiple entities to which we surrendered it for (we thought) a single purpose. Advocates of such unrestricted technology have asserted “You already have no privacy; get used to it,” and they expect the rest of us to see the issue in their terms, agree, and acquiesce to the continual sifting of the intimate details of our lives.

It is at this point that the analogies to previous eras are most salient. We have never enjoyed total protection from the technologies of the age. There has always been a means to invade private domains, steal property, and cause various sorts of damage. “Privacy” is not a by-product of technology, and it need not recede because technological means are rapidly advancing. Privacy is a product of the social compact, and it is as essential to the social condition as is the integrity

of the individual corporeal body. We preserve it by deciding that it should indeed be regarded as a fundamental right, and using the alternate technology at our disposal—the law, and its instruments of enforcement—to insure that the social compact is honored by all.

Freeman Dyson recently observed that the age of Darwinian evolution has closed, yielding to the dominance of the human species and the shift to social evolution. The emergence of the cyber-*döppelgänger*, of an electronic identity (or identities) that is distinct from and independent of our physical self, is an important facet of that social evolution, one that is only now beginning to be charted.

On two fronts, our electronic selves are frightening. At one level, they are but cartoon representations of our real selves, abstract records that represent a part, but not the whole, of who we are. At another, they are not “us” but rather someone else’s edited version of who we are. Our electronic selves are caricatures that serve not our purposes but those of other entities (often unknown and unrevealed to us). As such, they bind us with metaphysical chains that restrict our horizons and our futures.

An Imperfect Storm: The Privacy Wars

The Privacy Wars began in 2009 with the cloning of cell phones of a covert team of Department of Homeland Security operatives staking out California billionaire Serge Sourpuss, who had been falsely identified as a financier of the nascent pan-Islamic militancy. In a counterespionage coup worthy of the movies, the Personal Information Limits Front: Electronic Resistance (PILFER) sent false text-message commands complete with authentication codes to stakeout team members, luring them into embarrassing encounters with goop and slime and

cartoonish devices usually not seen outside daytime television shows. The incident was captured digitally by the DHS unit’s own cameras, which had also been cyjacked (cyber-jacked).

The Keystone Kops scenes of stealthiness meeting silliness were simultaneously web-cast, pod-cast to the next-generation EyePods, and jacked into several of the nation’s cable networks. It preempted critical moments of the season’s final episode of American Idol, whose broadcast was hijacked by PILFER for a second time.¹

A more serious blow was the subsequent posting of the DHS unit’s phone records and Blackberry files, worm-pulled from the secure service provider and similarly billboarded all over cyberspace. The phone records showed that the two “anonymous” phone calls that ostensibly provided the initial cause to open the inquiry (calls made to an Administration-friendly news entertainment blog called The Dregs Report) actually came from the unit itself.² Of far greater import, however, was the Blackberry information, detailing just how much of the billionaire’s supposedly secure information had been obtained covertly—and illegally—by the squad. The Weblines “Bug Brother Is Watching You!” appeared as wallpaper on the traveling web site.

Outrage over the emergence of a new “dirty tricks squad” poured fuel on a fire already smoldering from past abuses. The DHS unit chief’s media-bestowed *nom du guerre* of “Donald Cigaretti” invoked the ghosts of enemies lists and arrogance. Administration spokespersons’ attempts to justify the squad’s actions as a necessary counter-terror measure fell flat. Even friendly media representatives, using their real names, pointed out the absurdity of creating false enemies when so many real ones demanded the attention of the intelligence community.

By itself, the incident might have had the minor impact of brief embarrassment, like a lost

military laptop or a stolen SWAT team weapons van. However, it occurred three weeks after a similar widely publicized cyjacking of well-heeled donors to the Committee to Repeal the 25th Amendment at a fundraiser in Washington, D.C. While the cloning of cell phones had been identified as a security problem several years earlier with the theft of phone numbers from celebrities' cell phones, PILFER managed to crack state-of-the-art anti-theft devices that were installed in the cell phones of several government officials and "advisors" among the crowd (similar technology protected the cell phones of the DHS squad). The original Web-cast of the cyjacked information did not include the information stolen from the state-of-the-art phones: PILFER had not wanted to tip its hand to the DHS sting in California, which was still in its worm-pulling phase at the time.

The Wall Street Journal had trumpeted the protection of information of those individuals with the new cell phone technology (among whom were several "Pentium Plutocrats," chief executives of Internet and data-warehousing/data-mining companies) until Web- and Pod-casting services distributed a "Separated At Birth?" comparison the day after the California debacle. *The Journal* headline, the *Los Angeles Times* headline announcing the botched California raid, and the "protected" data were all available around the globe along with streaming video of the raid: PILFER withheld the protection-cell phone data from its original Washington release in order to maximize the Administration's embarrassment, anticipating that *The Journal's* response would come from someone.

Behind the scenes, as research in various archives has confirmed, the mining mavens were furious. Out of the public eye, their own oxen gored, the Pentium Plutocrats began a relentless campaign to increase federal penalties for data theft. Most

of the model legislation protected commercial databases against intruders, but without including comparable protections for individual "identity data." In keeping with earlier legislative initiatives, most of the bills contained provisions for insulating commercial data collectors, storers, and processors from lawsuits by individuals who suffered damages from data and identity theft.

The Rise of The New Populists

The administrative *faux pas* still might have died the natural death of all scandals had it not been so closely linked to the accelerating problem of identity theft. The ripple effect of the ChoicePoint, Bank of America, Wells Fargo, and military database scandals continued unabated on local, regional, national, and international scales. Under pressure from the Pentium Plutocrats, Congress had resisted calls to create a central database for tracking identity theft cases. No one could account for how many electronic identities had been compromised, how many times the known victims' data had been sold and resold around the world, or how much monetary damage had been inflicted. All attempts to quantify the problem were blocked by the data warehouses' claims that first, it was proprietary information, and second, such inquiry would seriously compromise their equally proprietary efforts to improve their protection of their customers' identities.

Then the media found their poster child: an educated, articulate, telegenic, middle-class widow of an Iraq War medal-winner who was evicted from her home because of financial difficulties stemming from unresolved identity theft. She had kept meticulous electronic records with hard-copy backup, supplemented by legally recorded tapes of her latter-day telephone conversations with industry representatives to whom she turned for resolution

of the problem. Despite her efforts, the legal limbo of her finances persisted until the home was repossessed.

When she turned to the media for help, she instantly became Anywoman. That nickname stemmed from her passionate declamation to Paula Zahn: “I have never been unemployed. I have never spent more than I earned. I have always taken the industry’s recommended precautions, and aggressively sought to upgrade my protection. I have been blessed with enormously supportive family and friends throughout these ordeals. And I am on the brink of losing everything because my identity was stolen and no one seems to be able to fix it. If this can happen to me, it can happen to any woman!”

As the news media filmed sheriff’s deputies moving her furniture to the sidewalk, Anywoman turned to the cameras with a blistering denunciation of the “ownership society,” excoriating the Congress for being in the pocket of the Pentium Plutocrats, and asking the rhetorical question “What are my alternatives so that this never happens again?”

That question ignited the blogosphere. More and more victims of identity theft came forward, highlighting more and more instances of industry inability (and in some cases, unwillingness) to correct the problems. The mainstream media lost control of the story, and were reduced to reporting on the contents of the blogosphere as the issue came to dominate the national conversation.

Populist candidates threw their hats into the ring of the upcoming elections, demanding a potpourri of additional computer security, restrictions on data-sharing, and avenues of recourse for victims of identity theft. Both traditional polls and the blogosphere showed them attracting a substantial minority of support for their essentially single-issue campaigns, and incumbent politicians began to propose bills to steal the issue from the populists.

The Industry Response

The data mining industry responded with assurances of higher-technology solutions, incorporating biometrics. They stayed on-message with reminders that none of the information “lost” was actually private (having been voluntarily surrendered in the first place and shared in strict accordance with the small print of agreement forms that the affected consumers had presumably read and understood), that identity theft had occurred even under paper-driven systems, and that the industry was working very, very hard to assure their customers. A smaller number attempted to make the case that “transparency” actually protected individuals because the more information that was available, the more it could be verified in the light-speed networks.

The Administration joined in the defense of the industry by linking the identity theft issue to homeland security’s long-stalled proposal for a national identity card predicated upon biometrics. A prototype was to be distributed on a voluntary basis, combining personal, financial, medical, and biometric scales similar to the DNA-based new-generation dog tags of the U.S. military. The U.S. Attorney General received the first prototype I.D. card in a prime-time Rose Garden ceremony, and made the historic first withdrawal of money (a modest fifty dollars) from a wireless ATM brought to the Rose Garden for the occasion.

Two days later, PILFER broad-, web- and pod-cast the Attorney General’s personal data, including her biometric security code. Accompanying it were the account numbers and passwords of the bank accounts PILFER had established with it in all fifty states and the Virgin Islands, under the name “Eli On” (for “E-Lie On...” according to PILFER’S announcement). Each account held a modest fifty dollars, electronically

transferred from the A.G.'s original account. The new account information was revealed "so that the Attorney General is not permanently deprived of her rightful property," according to PILFER's accompanying manifesto.³

The tabloid headline "Bluetooth Blew Truth" became the rallying cry of the then-amorphous resistance to a national ID card. Sensing blood in the water, the news entertainment media began running stories headlined "The Demise Of The World-Wide Web" and "What Is The Net Worth of The 'Net?'" The blogosphere became a cauldron of conspiracy theories, most of them intricately constructed more of fear than of fact.

An obscure academic in Ohio was asked by a reporter about the industry's assertion that electronic transactions were really no different than their face-to-face predecessors. His answer was picked up by the news wires, then by the blogosphere: "Some one has always known. What is different is that now, anyone and everyone can know." An anonymous blogger added "Transparency Is Privacy" to George Orwell's famous triad from 1984 ("War is Peace / Freedom is Slavery / Ignorance is Strength"), and the mantra spread like wildfire on bumper stickers, backpacks, and e-mail tag-lines.

A growing number of Americans decided that they did not wish to live in a glass house or a "transparent" society. While poll support for the populist candidates grew steadily, a grassroots economic self-help stratum quickly sprang up, spearheaded by credit unions and labor unions, and quickly joined by small banks. On-line tax filings to the IRS fell precipitously, replaced by paper reporting. A Senator who was a staunch advocate of the banking and data-mining industries introduced a bill attempting to amend the tax code by requiring electronic filing. This ignited a blistering torrent of e-mail and snail-mail, and the bill died in committee.

The European Union Electronic Underground (EU2) began mimicking the cyber-attacks of PILFER, with almost daily exposés and manifestos published under the *nomme du guerre* of its putative leader, Pro Bono. Though their exposés were heavily censored so as to minimize the jeopardized data (flirting with but not stepping over the European Union's own privacy laws), they had the desired effect: the American cyber-dilemma became the most visible topic in Europe as well, eclipsing the travails of England's royal families and drowning out the ramblings of the neo-Nazi movement. American corporations came under heavier criticism from the European Union for their shoddy protection of consumer data, with threats of boycott and a suit before the World Court to protect European citizens' transactions in accordance with European standards.

The Redefinition of Homeland Security

To no one's surprise, the data-mining industry's response to the turmoil was to link their lucrative business to homeland security. Flogging the concept of "transparency" as a defense against both identity theft and terrorism, they continued to maintain that no changes could be made to their business without catastrophe occurring. However, in a particularly acrimonious face-to-face exchange with an industry flack during a rally on the Mall, Anywoman changed the debate with a single question: "How can the homeland be secure when the home is not?"

That question effectively ended the first round of the privacy wars, and redefined the terms of the debate. A new discourse began, instigated in cyberspace and quickly distributed by neighborhood-based papers that served areas with little or no Internet access. A code of civility evolved around an initially small debate among three primary bloggers: General Net Ludd (presumed by many

to be either the de facto leader or the collective avatar of PILFER), a conservative industry defender whose cybername was ALLCAPP (like his posts, which carried the tagline: “WHAT’S BAD FOR GENERAL BULLMOOSE IS BAD FOR THE U.S.A.”), and Phydeaux (“In cyberspace, nobody knows you’re a dog,” the caption of an old New Yorker cartoon) who represented the vast majority of users concerned about the short- and long-term implications of data-sharing and identity theft, but bewildered by the rancor of the debate.

One of the CEOs of the computer industry sponsored an open forum, PlebiSite, initially inviting the three primary spokespersons to refine the edges of the debates with a blog entry each week. Their three-way dialogue quickly accelerated to an entry each day, which drew the attention of hackers. The nominally secure site, open to the three invited participants but read-only for the general public, was quickly stripped of its security devices by Kan Key-See and The Merry Phreaksters.

Intended to be a three-way debate, PlebiSite immediately became an open forum that served as a clearinghouse of public concern. Anywoman joined the three main spokespersons on occasion, but most of the input came from short, pithy statements or questions from citizens on all sides of the issue.

The anonymous blogger who adopted Legion as his or her cyber-name (“For we are many”) took the first step toward reorienting the public’s consideration of the privacy issue by invoking the Preamble to the Constitution: “provide for the common defense and ensure domestic tranquility.” Reminding the nation that the two attacks on the World Trade Center had been mounted because of its symbolic role as the center of the American economy, Legion offered a series of rhetorical questions about the impact of the globalizing economy on the average American. Net Ludd and Anywoman seized on those questions to

leverage their own attacks on the government and the financial community’s use of consumer data, respectively, and Legion’s input was swiftly shunted aside into a sidebar thread.

The mainstream media deemed the resulting exchange of views “the new national conversation,” and began to track its themes. Concern over the manipulation of personal data replaced tirades about “privacy” (ironically mimicking earlier rhetoric from aborted attempts to redefine Social Security as “private” and “ownership”). Six segmented dialogues ensued, focusing on the resale of information surrendered for credit; medical information; public surveillance by private entities and corporations; covert surveillance by the government acting on probable cause; similar surveillance by government entities in a “proactive” role, which incorporated the idea of a national ID card; and the industries of data-mining and academic research.

The surveillance debate flared intensely at first, fueled by one of the ACLU’s perennial challenges to a local police department’s practice of videotaping political demonstrations. ALLCAPP challenged the ACLU to cite any cases since 1984 when such videotaping had led to any prosecutions, or even curtailments of individuals’ right to freely assemble, speak, or petition their government for redress. Phydeaux deflected the issue somewhat by pointing out that the same practice had also helped bring to justice several serial arsonists, the provocateurs who had attempted to turn peaceful protests violent on at least one occasion, and scores of individuals who had committed serious acts of assault and vandalism during violent protests against the WTO and other international bodies.

Then one of the outspoken proponents of surveillance proposed that CCTV be installed in public toilets “to protect the unborn” by documenting the abandoning of newborns. The resulting flame war led to monitoring of the

PlebiSite postings, and to self-moderation by the remaining posters. After a renowned Harvard-based attorney posted a synopsis of the Supreme Court cases dealing with privacy, most accepted the lack of privacy in public space and the workplace, as well as the government's overriding interest in conducting surveillance for criminal cases. A trailing debate over the permanence of records and the limits on dissemination of images merged with the larger umbrella of medical and credit privacy.

Credit Information. Given the pervasive need to use credit in modern society, this debate soon turned on whether credit information should be established on an Opt-In or Opt-Out basis. ALLCAPP stayed on-message for the industry mavens, touting the "opportunities" that would result for consumer and industry alike if credit information could be shared. He stridently advocated for the current status quo of Opt-Out, invoking images of Jeffersonian yeomen farmers being informed and advised of the things that concerned them and their government.

Net Ludd countered with a salvo of federal laws and their corresponding regulations, in brief, asking rhetorically how anyone who actually worked for a living could individually manage to stay abreast of developments that highly-paid specialists tracked for industry. He argued for simplicity from the consumer's side: Opt-In allowed those who wanted to be contacted to participate, but the default stance should be that the consumer had an equal stake in the purchase of credit with the provider of credit. Their proprietary relationship should be limited as a matter of law to that purchase, and extend no further.

After a flutter of postings asking if Ludd "worked for a living" himself, ALLCAPP responded with lengthy summaries of credit defaults, bankruptcies, and delinquencies. Those abuses of credit, he argued, made data-sharing mandatory. Phydeaux countered with a mild question of whether

anyone knew how many of the bankruptcies resulted from identity theft.

In response, PlebiSite was flooded with posts from individuals who had suffered financial losses from both identity theft and uncorrected errors in their credit reports. A second wave of new participants followed a week later, after the mainstream media picked up the story. Additional horror stories about criminal histories established under stolen identities began to sprinkle the discussion.

Medical Information. A parallel thread, at first unconnected to the identity theft discussion, had been muted until the flood of identity theft stories. The medical discussion then shifted from hypothetical Gattaca-like denials of insurance coverage and employment opportunities. Many contributors reported receiving advertising for medications directly related to conditions they had thought were known only to their physicians.

Four separate mainstream media outlets jumped on the new thread, pushing several long-term investigative reporting efforts into the spotlight. The interconnected associations of the medical, pharmaceutical, and insurance industries centered on several of the high-profile data-mining corporations already being pilloried in the credit and identity theft threads.

The untimely death of one of the representatives from a western state intervened. Six vocal privacy advocates filed as independent candidates in a special election held to fill his office, but early poll returns indicated that business-backed candidates from the major parties were profiting from the split vote for the opposition. The second-leading privacy candidate withdrew in favor of the issue's front-runner, giving a bravura performance that clearly wrote the privacy agenda's manifesto for the state's constituents. Several other privacy advocates followed suit, giving the privacy slate a

strong plurality.

The overall economy of the state was healthy, individual bankruptcies and a series of farm foreclosures in the northern part of the state elevated data privacy to the signature issue of the election. Though party representatives attempted to define the election as a two-way race based on family values, the media and the blogosphere kept the privacy issue, and the independent candidacy, at the forefront. Behind a series of ad hominem attacks against the Independent, the major party machines quietly conceded the ground, and responded. They launched a heavily funded campaign against any restrictions on current business practices, dominating the mainstream airways but thoroughly derided and lampooned in cyberspace.

In the only three-way debate among the major candidates, on the eve of the election, both party candidates gave strong defenses of existing privacy practices, only to see their supposedly private data highlighted on the screen behind them: PILFER had engineered another cyjacking.⁴

The following Tuesday, the independent candidate won more than 53 percent of the votes cast, in an election notable for its high turnout. The mainstream media trumpeted the victory as a mandate for privacy, noting that there were no other high-profile stakes in the election. Upon arriving in Washington, D.C., the newest representative immediately filed a PILFER-designed bill that gave control over individual data to the individual, and required specific permissions for any data sharing. All secondary recipients of data, whether credit bureaus or insurance companies, would be bound by the specific requirements of the primary surrender of data.

Within 72 hours, the bill was festooned with amendments that eviscerated the spirit of the bill, promoted on the basis of “transparency,” though there was little evidence of anything behind them

but exempting the data industry from the main provisions of the bill. The House leadership rushed the bill to committee for a vote.

The network of privacy advocates that had evolved from the PlebiSite discussions anticipated such a reaction. Congress-watchers wirelessly blogged each of the amendments almost as soon as it was offered. Snippets of each sponsor’s proposal and speech filled the blogosphere, and a flood of e-mail and snail mail filled congressional mailbags and inboxes, railing against the changes. The Independent withdrew the bill with a flourish in a media-heavy press conference, excoriating the added provisions and gently chiding their sponsors.

A network of political operatives with ties to billionaire Sourpuss (but not to PILFER) quickly filed recall petitions against amendment sponsors in every jurisdiction where recall was available. The recall petitions were supplemented by a rash of independent filings for the upcoming congressional races across the country. Under this unanticipated pressure from privacy advocates, few in the national legislature were willing to support openly any bills supporting unrestricted data sharing.

The various state-based privacy coalitions united under an umbrella group formed in Maine, PRIVAC-E, allowing Sourpuss and PILFER to remain apparently peripheral to the larger movement. Though he channeled some funds to PRIVAC-E through above-board means, Sourpuss saw the advantage of a grassroots organization that had plausible deniability in case PILFER’s underground campaign was exposed. PILFER returned to Fifth Column status, staying out of the public eye until the anticipated counterattack by the data industries and their allies.

The Counterattack

The final stages of the battle were fought in the run-up to the mid-term election. When the discussions of identity theft problems faltered on PlebiSite, the data mining industry launched a media blitz promoting “transparency” as a means of preventing and surviving identity theft and other misuses of personal data. A spate of industry-sponsored posters filled PlebiSite with messages that hawked the inevitability of identity theft problems under the ineffectual patchwork of laws and regulations that plugged holes well after the fact. Talk shows were suddenly filled with “experts” who pronounced the old notions of privacy dead, the inevitable casualties of the globalization of the economy. The message was consistent: only full exposure, in multiple locations that could be checked and verified at lightning speed, could thwart attempts to purloin or alter personal data. The industry promoted the potential benefits to the economy that would be derived from reducing fraud, hinting at lower consumer prices across the board, from retail to auto insurance to medical insurance.

At the same time, Administration supporters of the industry brought forth a series of initiatives under the banner of homeland security. A series of cases of attempted terrorist assaults that allegedly were intercepted or otherwise neutralized were promoted in news conferences. Spanning almost a full decade, from the months immediately following the 9/11 attacks to December of the preceding year, the incidents were linked by assertions that data mining had led to the identification of the terrorists. The consistent message was that the ability to sift through credit card transactions, cell phone traffic, library and Internet use, and in one case GPS tracking of a rental vehicle had kept America safe. An underlying theme hinted that the same techniques were protecting Americans from criminal activity.

PILFER had anticipated the general outlines of the industry’s campaign, but held back its response for several weeks. During that time a blizzard of objections filled the blogosphere and dominated traffic at PlebiSite, a vociferous if uncoordinated vox populi rebuff of the industry’s and the administration’s assertions. The tail wagged the dog at first: most of the early posts ignored the covert tracking of terrorists (of which the general public knew nothing) and focused on the identity theft issue that they knew only too well. A radical economist who had been employed in several Ivy League schools commandeered an outdated advertising slogan—“I am the C.E.O. of Me!”—to put forth a strident philosophical view that by advantaging corporate use of personal data, the administrations of several presidents had undermined the economy by suppressing both control and decision-making, and thus creativity, at the most important level of the economy. No one paid any attention to the convoluted economic proofs offered by the economist, or to the more well-grounded rebuttals from mainstream economists, but the slogan quickly became the rallying cry of the opposition.

By trying to hijack and redirect the national discussion, the industry inadvertently highlighted the pervasive encroachments upon personal privacy, and reignited the moral indignation of the citizens watching the unfolding drama. A couple of the new PlebiSite contributors who were on the industry payroll were outed by a freelance whistle-blower who had once worked in the industry. She posted memos outlining industry plans (created several years earlier) for a “transparency” campaign in case Congress ever brought pressure as it had against the tobacco industry: some of the wording of that campaign’s “Concerned Citizen Letters” were identical to posts on PlebiSite.

Industry spokespersons began an immediate

campaign to discredit the whistle-blower as a disgruntled employee, hinting that she herself had posted the CCLs she criticized. They also attempted to turn her message back on itself, asserting that transparency rules, the industry's participation in the debate through their agents would have been widely known and thus no scandal whatsoever.

PILFER held back until the character assassination reached a peak, then unleashed a barrage of intra-industry communications provided by moles within the industry (some were in fact disgruntled employees; others were PILFER operatives who had worked in the industry for years, including one of PILFER's founders). At the same time, PILFER posted pending legislation that purported to provide transparency protection, detailing the ramifications of each and every provision that alleged consumer protection, but actually constituted insulation of the industry against lawsuit by consumers.

Putting the data industry under a microscope was bolstered by a general exposé of existing laws and proposed legislation that impeded inquiry into corporate finances and deal making. The slow swell of stealth legislation, riders, and amendments that had undone most of the Sarbanes-Oxley law had been the original issue around which PILFER had organized, and it had extensive files with clear-cut points of attack.

Integrating fragmented investigation by a score of smaller citizen advocacy groups, PILFER jumped on the "CEO of ME" bandwagon. In its most mainstream publicity campaign to that point, PILFER hammered home the discrepancies between the protections afforded the Pentium Plutocrats and their corporate brethren, and the exposure in the name of "transparency" that was inflicted upon the citizens of the nation. The campaign morphed the CEO image into a new slogan, "With Transparency and Justice For All," demanding that

the corporations be subjected to the same levels of transparency as the citizen "Me-E-Os." After two weeks of bulleting the disparities, PILFER put forth model legislation for achieving just that. Sitting members of Congress were swift and almost unanimous in their denunciation of the model legislation, which essentially meant that PILFER had promulgated the platform of the opposition in the coming election.

The provisions of the nascent Patriot Act V were also dissected, outlining the two-pronged assertion of increased federal snooping power and restrictions upon Freedom Of Information provisions. Anywoman's "how can the homeland be secure when the home is not?" question dominated the debate, however: most citizens could find common ground with those whose lives had been thrown into turmoil by data theft and misuse, where they had little emotional connection with government intrusion. Nevertheless, it remained an important, and strident, sub-thread that periodically augmented the more personal discussions on credit and medical histories. As one historian has noted, looking backward on the period, the FOIA thread continually reminded citizens of the role government had played in allowing the credit situation to evolve, and of the obstructions it had placed on ordinary citizens' ability to regain control over their lives. While few bought into the more revolutionary claims that the national government was a wholly-owned subsidiary of business, many recognized and remarked upon the need to control government in order to control business excesses.

A week before the elections were to be held, Legion rejoined the debate, posing the question, "What becomes of 'private property' if there is no privacy?" She or he drew out the invisible threads of the industry proposals, noting that all of them contained a tacit assumption that information about a customer or client constituted the agency's

“proprietary” property—a word, Legion noted, whose dictionary definition meant “ownership.” Legion then posed the second, more important question: “When did I become a slave? That so-called ‘proprietary’ information is an electronic version of me, and it is available to be bought and sold... not down the river, but down the data stream. How is it that they have such control over me, and I do not? In this matter, I think, Anywoman and I have common cause: allowing our electronic selves to be converted to others’ property nullifies our autonomy, effectively cancels our citizenship, and renders us slaves, not to a plantation master, but to corporate interests. And yet we are supposed to have a constitution that prohibits slavery. The time has come, to reassert our rights as free men and women. We know that the technology exists that makes this possible. The technology also exists to make armed robbery possible. We prohibit that misuse of hard steel technology, and it lies within our power to prohibit the misuse of electronic technology.”

Merged with the “CEO of Me” campaign, Legion’s questions dominated the remaining blog traffic on the election’s eve. The populist candidates seized on the issue, and pushed out rapid position papers reaffirming the individual’s right to be protected from electronic slavery. PRIVAC-E sponsored agile sound-bytes highlighting the difficulties individuals had experienced in regaining control over their finances, highlighting the exceptional deference that business gave to their electronic profiles and faux histories, with little or no regard for the real-world (paper) evidence that was provided by real-world people. The industry replies (detailing instances of fraudulent claims, among other things) were strongly worded and well-documented, but fewer in number than the horror stories that PRIVAC-E summarized and re-posted.

And then, on a clear, bright day in early November, America awoke, and went to the polls.

Endnotes:

¹ *American Idol* was targeted after ostentatious announcements by the various network and cable executives that the infamous spoof episode “*America, I’m Dull*” could never happen again. In fact, a ‘deja view’ was already in the works for an episode of *The Simpsons*, titled “*America, I’m - D’OH!*” Although PILFER was publicly blamed for the original broadcast override, the group never took credit for it, and the cast of digitally-disguised characters on the show spoke and “sang” with accents that suggested a Slavic origin.

² The fact was that the phones had already been cyjacked by PILFER, who made the instigating calls without the DHS unit’s knowledge. The cyjacking took place in response to the original intrusion into Sourpuss’s records. Although the “information” about the pan-Islamic financing in the files was false—the investigation team actually hacked a honey pot that Sourpuss and PILFER established before the billionaire began his public campaign against the Administration’s Middle East policies—the fact of the intrusion took on dimensions greater than its individual merits. Sourpuss was never prosecuted for the alleged bankrolling of “terrorists,” and the federal government failed to substantiate any of the nominal leads provided in the honey pot. The full story would not be revealed until Sourpuss’s death in 2011, by which time the California incident had become the Blitzkrieg of a new cyber-war against perceived abuses both public and private, and PILFER felt secure enough to acknowledge that in fact Sourpuss was bankrolling PILFER, not the pan-Islamic movement.

³ Intent to permanently deprive the rightful owner of property is an essential mens rea element of the crime of theft, so PILFER’s street theater had a self-serving element as well.

⁴ Though all three candidate’s finances were bared, the Independent candidate was a private citizen of modest means, with very little to hide. He had offered to make the information public early in his campaign, as an “I have nothing to hide and I still want my privacy!” gambit. He was contacted by PILFER almost immediately, and as his candidacy grew, the monkey-wrenching plan was conceived.

References

Dyson, Freeman. (2005). *The Darwinian Interlude*. Retrieved from < <http://www.technologyreview.com/articles/05/03/issue/magaphone.asp> > 3 March 2005.

Feuer, Alan, and Jason George (2005). “Internet Fame Is Cruel Mistress for a Dancer of the Numa Numa.” *The New York Times*. Retrieved from < <http://www.nytimes.com/2005/02/26/nyregion/26video.html> > on 26 February 2005.

Reuters (2003). *No Surveillance Tech for Tampa*, Retrieved from < <http://www.wired.com/news/politics/0,1283,60140,00.html> > on 21 August 2003

Afterword

Michael E. Buerger

The future is often regarded as the realm of visionaries, prophets, and science fiction writers. It is also the province of planners, those who have an understanding of how the threads of the past have woven the future, and sufficient foresight to see the possible ways those patterns may continue beyond the present day. Unlike dreamers -- who may muse, "What if...?" and speculate about those possibilities -- planners ask "What if...?" and work to bring the best possibilities into reality.

The Futures Working Group encompasses dreamers and planners alike. In the short term, we each work in our respective areas to craft effective change, anticipating and meeting the challenges of the near future. Over the longer term, we engage in informed speculation about the impact of larger trends, considering both preferred and adverse developments. In the latter area, we examine more abstract possibilities, laying the groundwork for shaping and responding to trends and events beyond our immediate sphere of influence. The evolutionary change of Levin and Jensen's contribution is similar to Myers' and Melis's "Wild Cards," which nevertheless embody differences akin to the overnight introduction of new technologies. These shifting possibilities produce a constant stream of change, each of which forces us to adapt, question, and reconsider what we once accepted as fact, and to look beyond the comfortable understandings of what is to the more uncertain realm of what might become, and be coming.

In doing so, we take guidance and inspiration from those whose profession is the future: from Alvin Toffler, who inspired the first Futures course at the FBI Academy, to John Smart, whose presence and contributions inspired us at our meeting in Phoenix.

The work of John Smart and of Richard Clarke provided direct inspiration for this volume of the Future Working Group's papers. Several of this volume's authors note that envisioning our world ten years into the future takes us well beyond the familiar near-term future that is the focus of our "day jobs." As a result, working independently of one another, we evoke multiple possibilities, interweave common and diverse themes, and arrive at vastly different visions of the world in 2015. We have indulged in more fanciful imaginings for this volume than is our usual fare, with results we hope are both entertaining and thought-provoking.

We have not explored all the possibilities, nor asked all the questions that we might have. Many of those questions will evolve over time, and may provide the grist for future volumes of the FWG:

- Can government logistics at any level (but especially at the local level) keep pace with the accelerating change of technology, and what are the implications for governance if not?
- Will the New Luddites be technophobes, or scientifically sophisticated enough to infiltrate and destroy systems from within?
- What recourse is available to an armed but polite society against the predatory mechanisms of the sophisticated online banditry, operating from halfway around the globe?
- Is human nature malleable enough, or sensible enough, to make the cognitive shift from "number of persons robbed this year" to a SEAP model of "number of persons not imposed upon by crime"?
- How would a loosely-linked network of Ted Kaczynskis work, and what kind of havoc could they wreak?

Is it possible to broaden the use data-mining from the identification of toxic individual patterns to the identification of toxic local trends, in support of SEAP goals? Will there be enough political will to make such a transformation?

Is a polite but armed society only possible in places already polite and relatively homogeneous, like Smallsville?

What are the implications of being “an agent of the State” in an era of increasing privatization, and/or of accelerated marginalization of nation-state governance?

How will the Smallsvilles of the nation and the world react to the imposition of outside pressures, whether economic change or ethnographic and cultural changes wrought by migrations?

Will biometrics prove to be the salvation of electronic commerce, or merely a longer string of ones and zeros to be stolen, compromised, altered, and suborned?

How many variations of the Smallsville self-policing model might evolve if the public police of today disappear as a legitimate enterprise? Is the likelier result a broader democratic network, or a return to social Balkanization?

What social dislocations and individual adaptations can we anticipate if privacy becomes impossible in fact, and transparency is imposed upon the populace by fiat, either by evolutionary change or developmentally?

These and many other questions remain, and more will emerge from the process of trying to answer them. The published works of the Futures Working Group began with the idea of localized nodes of self-governance, and hence police work: the Smallsville model of this volume. The other

pieces in Volume 1 were responses to that central idea.

In this work, Volume 2, that concept serves as a springboard for a longer leap of faith and supposition, and an exploration of broader themes. The questions and possibilities depicted in these essays may be considerably more salient if we revisit the issues in five years’ time; some may have achieved considerable resolution—politically, a National ID card may be a reality within that time, or the idea may have been banished—and the others will be entwined with new, emerging issues.

Subsequent volumes planned for the Futures Working Group return to the focus on a common theme. The third volume follows on the heels of Hurricane Katrina and the centennial anniversary of the San Francisco earthquake. The essays will examine the future demands and needs of disaster preparation. The fourth volume will revisit a theme raised in this volume by several authors: the merging trends of militarization of police operations, and the military’s adaptation to a post-invasion policing role. That volume will also address changes in the intelligence community, and the potential impacts for the American police.

In this as in all our other works, we hope to inspire and challenge. We invite responses, whether in agreement or rebuttal, and invite any and all interested readers to join in the ongoing effort to create a better future.

About the Authors

Sandy Boyd is Professor of Administration of Justice at College of Marin in Kentfield, California. Dr. Boyd is also adjunct faculty for Excelsior College, teaching undergraduate Criminal Justice, Psychology and Sociology. For Capella University, Dr. Boyd teaches in the doctoral program in Education

Michael E. Buerger is Associate Professor of Criminal Justice at Bowling Green State University in northwest Ohio. He has been a municipal police officer in New Hampshire and Vermont, and directed police research projects in Minneapolis and New Jersey. Dr. Buerger is a member of the Futures Working Group.

Thomas J. Cowper is a 23-year law enforcement veteran who has held various patrol, administrative, training, management, and executive positions within his agency. Since 1995 he has been involved with technology procurements for law enforcement and the management of public safety radio system programs in his state. He is the current 1st Vice President of the Society of Police Futurists International and a member of the Futures Working Group. He is a graduate of the FBI National Academy, has a BS in Mechanical Engineering Technology from LeTourneau University, and a master's degree in Public Administration from Marist College. He speaks and writes extensively on issues concerning technology and its impact on law enforcement and government.

Charles "Sid" Heal has been in law enforcement 31 years and is currently a Commander with the Los Angeles Sheriff's Department. During his tenure he has been involved in nearly all facets of

law enforcement. He has three college degrees and is a graduate of the FBI National Academy and the California Command College.

Carl Jensen is a Supervisory Special Agent currently assigned to the FBI's Behavioral Science Unit. In addition, he is the Chairman of the Futures Working Group, a collaboration between the FBI and the Society of Police Futurists International. In his career with the FBI, Dr. Jensen has served as a field agent in the Atlanta and Youngstown, Ohio, offices and as a Forensic Examiner in the FBI Laboratory. Prior to joining the Bureau in 1984, he served in the Weapons Department aboard a nuclear fleet ballistic missile submarine.

Bernard Levin is department head/psychology at Blue Ridge Community College. He has worked in laboratory, law enforcement, correctional and other organizational settings, and has led a variety of professional and civic organizations. At present, he is director, research and development, of the Society of Police Futurists International and vice chairman of the Futures Working Group. He also serves as visiting scholar at the FBI Academy and is commander, policy and planning, at the Waynesboro Virginia Police Department.

Alberto Melis is currently the Chief of Police in Waco, Texas. Prior to that he was Chief of Police in Lauderhill, Florida, just after serving 24 years with the Delray Beach Police Department, also in Florida. He is a member of the IACP Community Policing Committee, active in PERF and among other things participated in the national evaluation of the 1994 Title One Crime Bill

Richard W. Myers has served as Chief of Police for the City of Appleton, Wisconsin since 1995. He has previously served as police chief for communities in suburban Chicago and his native

state of Michigan. He began his career in policing in 1977 and has held varying appointments, such as police officer, deputy sheriff, public safety officer (police and fire), and Medical Examiner Investigator. Myers is a graduate of Michigan State University (BA and MA), the FBI National Academy (156th Session, 1989), and the FBI LEEDS Seminar (26th Session, 1992). His leadership experiences include past Presidencies of the Wisconsin Chiefs of Police Association, the Society of Police Futurists International (PFI), and the Wisconsin Police Executive Group. Myers was a Charter Member of PFI, as well as an original member of the Futures Working Group.

Dr. Andreas (Olli) M. Olligschlaeger is the president of TruNorth Data Systems, Inc., a company specializing in law enforcement information systems consulting and software development for federal, state and local agencies. Formerly a systems scientist at Carnegie Mellon University, with appointments at the H. John Heinz III School of Public Policy, the Robotics Institute and the School of Computer Science, Dr. Olligschlaeger also has practical experience working with law enforcement agencies in narcotics enforcement, crime analysis and criminal intelligence. The primary focus of his work is on artificial intelligence methods for crime forecasting, advanced analytical tools for the automated mining of very large data sets for both crime analysis and criminal intelligence, advanced spatial statistical methods for geographic information systems and crime mapping, and the development of law enforcement related systems that integrate many different analytical techniques into a single interface. Dr. Olligschlaeger is a member of the International Association of Crime Analysts, the International Association of Law Enforcement Intelligence Analysts, the Society of Police Futurists International, the PFI/FBI Futures Working Group and serves on the advisory board of the High Tech

Crime Consortium. Dr. Olligschlaeger holds a B.A. in Geography from Concordia University an M.A. in Geography from the University of British Columbia, an M.Phil. in Public Policy from Carnegie Mellon University, and a Ph.D. in Public Policy, also from Carnegie Mellon University.

Joseph Schafer is Associate Professor in the Center for the Study of Crime, Delinquency, and Corrections at Southern Illinois University Carbondale. He is a graduate of the University of Northern Iowa and Michigan State University. Dr. Schafer is actively involved in researching police organizations, police behavior, and police operations. He is the author of *Community Policing: The Challenges of Successful Organizational Change* (LFB Scholarly: 2001). Dr. Schafer is President of Police Futurists International and a member of the Futures Working Group.

Alan Youngs is a former division chief of the Lakewood, CO police department, where he served for 33 years. He is currently a practicing attorney and a law enforcement and security consultant residing in Colorado. He is past-president of Police Futurists International and a member of the Futures Working Group.



U.S. Department of Justice
Federal Bureau of Investigation

PRSR STD
POSTAGE & FEES PAID
Federal Bureau of Investigation
Permit No. 168

Futures Working Group
Behavioral Science Unit
FBI Academy
Quantico, VA 22135

Official Business
Penalty for Private Use \$300

