The Best Laid Plans: An Assessment of the Varied Consequences of New Technologies for Crime and Social Control

Author
M. Byrne, James

Published
2008

Journal Title
Federal Probation

Rights statement
© The Author(s) 2008. The attached file is reproduced here in accordance with the copyright policy of the publisher. For information about this journal please refer to the journal's website or contact the author.

Downloaded from
http://hdl.handle.net/10072/50631

Link to published version

Griffith Research Online
https://research-repository.griffith.edu.au
The Best Laid Plans: An Assessment of the Varied Consequences of New Technologies for Crime and Social Control

James M. Byrne, Professor
Department of Criminal Justice and Criminology
University of Massachusetts, Lowell

TECHNOLOGICAL INNOVATION is a double-edged sword in the field of criminal justice. It has the potential to dramatically improve both the efficiency and the effectiveness of the criminal justice system; but it also has the potential to divert critical resources away from more traditional crime prevention and control strategies that may actually make us safer, without the negative side effects (such as erosion of personal freedom, increased public distrust, and emphasis on coercive control). Recent changes in the technology area generally—and in the area of information technology in particular—have been so dramatic and profound that they deserve special attention and critical review. Technological advances and innovations have been decried by some as a cause of crime and embraced by others as a solution to our crime problem. As I demonstrate in this article, it is important to consider new technology both in terms of crime causation and crime prevention and control, because if history is our guide—and in this case it needs to be—there will invariably be both intended and unintended consequences for any new technological innovation in each area (Marx, 2007).

It is my intent to provide readers with an examination of a wide range of new technological innovations that have applications in the areas of crime commission, crime prevention, and crime control (by police, courts, and corrections). In presenting this review, I offer a description of recent technological innovations, along with my preliminary assessment of the impact—both intended and unintended—of each form of new technology, while also exploring the key issues. As I consider each of these hard and soft technology applications in the field of criminal justice, it is certainly possible to think of how individuals or groups could utilize some of these same technological innovations to commit crimes and/or support ongoing terrorist activities. Indeed, this is precisely the rationale underlying the FBI's assessment of our country's cyber crime problem: Cyber threats confronting the United States emerge from two distinct areas: (1) traditional criminal activity that has migrated to the Internet, such as fraud, identity theft, child pornography, and trade secret theft; and (2) Internet facilitated activity, such as terrorist attacks, foreign intelligence threats, and criminal intrusions into public and private networks for disruption or theft. The vulnerability of the United States to such activity is rapidly escalating as its economy and critical infrastructures become increasingly reliant on interdependent computer networks and the World Wide Web. (FBI Strategic Plan, 2004, as summarized in Byrne and Rebovich, 2007:5)

It appears that advances in both hard and soft technology have resulted in new opportunities for crime (through the internet), new forms of criminality (e.g. Internet scams, sex crimes on the Internet), new techniques for committing crimes (e.g. computer software programs, pirating, and extortion; the use of tasers as weapons in robberies), and new categories of offenders and victims (such as

2. The New Technology of Crime

Innovations in criminal justice technology can be divided into two broad categories: hard technology (hardware) and soft technology (software/information systems). Hard technology innovations include new materials, devices, and equipment that can be used to either commit crime or prevent and control crime. Soft technology innovations include new software programs, classification systems, crime analysis techniques, and data sharing/system integration techniques that also provide opportunities for both crime commission and crime control. Table 1 highlights the types of hard and soft technology innovations in crime prevention, policing, the courts, institutional corrections, and community corrections (adapted from Byrne and Rebovich, 2007).

Although this listing of new hard and soft technologies is not meant to be exhaustive, I suspect that it captures the range of technological innovations currently being applied in police, court, corrections, and community crime prevention programs, both in this country and abroad.

1 March 28, 2008 presentation at the 2008 Hixon-Riggs Forum on Science, Technology and Society, Harvey Mudd College, Claremont, California.
TABLE 1:
The Application of Hard and Soft Technology to Crime Prevention and Control

<table>
<thead>
<tr>
<th>HARD Technology</th>
<th>SOFT Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crime Prevention</td>
<td>Threat assessment instruments</td>
</tr>
<tr>
<td>- CCTV</td>
<td>Risk assessment instruments</td>
</tr>
<tr>
<td>- Street lighting</td>
<td>Bullying ID protocol</td>
</tr>
<tr>
<td>- Citizen protection devices (e.g. mace, tasers)</td>
<td>Sex offender registration</td>
</tr>
<tr>
<td>- Metal detectors</td>
<td>Risk assessment prior to involuntary civil commitment</td>
</tr>
<tr>
<td>- Ignition interlock systems (drunk drivers)</td>
<td>Profiling</td>
</tr>
<tr>
<td>Police</td>
<td>Crime mapping (hot spots)</td>
</tr>
<tr>
<td>- Improved police protection devices (helmets, vests, cars, buildings)</td>
<td>Crime analysis (e.g. COMPSTAT)</td>
</tr>
<tr>
<td>- Improved/new weapons</td>
<td>Criminal history data systems enhancement</td>
</tr>
<tr>
<td>- Less than lethal force (mobile/riot control)</td>
<td>Info sharing w/in CJS and private sector</td>
</tr>
<tr>
<td>- Computers in squad cars</td>
<td>New technologies to monitor communications (phone, mail, internet) to/from targeted individuals</td>
</tr>
<tr>
<td>- Hands free patrol car control (Project 54)</td>
<td>Amber alerts</td>
</tr>
<tr>
<td>- Offender and citizen IDs via biometrics/fingerprints</td>
<td></td>
</tr>
<tr>
<td>- Gunshot location devices</td>
<td></td>
</tr>
<tr>
<td>Courts</td>
<td>Case flow mgt systems</td>
</tr>
<tr>
<td>- The high tech courtroom (computers, video, cameras, design features of buildings)</td>
<td>Radio frequency identification technology</td>
</tr>
<tr>
<td>- Weapon detection devices</td>
<td>Data warehousing</td>
</tr>
<tr>
<td>- Video conferencing</td>
<td>Automation of court records</td>
</tr>
<tr>
<td>- Electronic court documents</td>
<td>Problem-oriented courts</td>
</tr>
<tr>
<td>- Drug testing at pretrial stage</td>
<td></td>
</tr>
<tr>
<td>Institutional Corrections</td>
<td>Use of simulations as training tools (mock prison riots)</td>
</tr>
<tr>
<td>- Contraband detection devices</td>
<td>Facial recognition software</td>
</tr>
<tr>
<td>- Duress alarm systems</td>
<td>New Inmate classification systems (external/internal)</td>
</tr>
<tr>
<td>- Language translation devices</td>
<td>Within prison crime analysis (hot spots; high rate offenders)</td>
</tr>
<tr>
<td>- Remote monitoring</td>
<td>Info sharing with police, community, victims, and community-based corrections (reentry)</td>
</tr>
<tr>
<td>- Perimeter screening</td>
<td></td>
</tr>
<tr>
<td>- Less than lethal force in prison</td>
<td></td>
</tr>
<tr>
<td>- Prison design (supermax)</td>
<td></td>
</tr>
<tr>
<td>- Expanded use of segregation units</td>
<td></td>
</tr>
<tr>
<td>Community Corrections</td>
<td>New classification devices for sex, drugs, and MI offenders</td>
</tr>
<tr>
<td>- GPS for offender monitoring and location restriction enforcement</td>
<td>New workload software</td>
</tr>
<tr>
<td>- New Devices (breathalyzers, instant drug tests, language translators, plethysmographs)</td>
<td>New computer monitoring programs for sex offenders</td>
</tr>
<tr>
<td>- Polygraph tests (improved)</td>
<td>Info sharing with community, police, treatment providers (for active offender supervision, and for absconder location)</td>
</tr>
<tr>
<td>- Laptops/GPS for line staff</td>
<td></td>
</tr>
<tr>
<td>- Reporting kiosks</td>
<td></td>
</tr>
</tbody>
</table>

There is obviously much more to discuss in this area (see Schlegal & Cohen, 2007; Taylor, et al., 2006), but I mention the technology of crime here to make a simple point: advances in both hard and soft technology have not been restricted to the criminal justice system's response to crime; they have also influenced criminal behavior in ways that are important to understand. I include some examples below of technology-related criminal behavior, using a typology originally offered by Richard Sparks (1980) to differentiate various forms of criminal activities as follows: 1) crime at work, 2) crime after work, and 3) crime as work. One development that bears closer scrutiny is the extent to which private sector companies may be marketing technology (new weapons/tasers and/or various surveillance software come to mind) to both criminal justice agencies and the general public. Similarly, the same companies contracted to protect the privacy of criminal justice data (e.g. data warehousing) may also be involved in selling information to the public included in these data bases (Rebovich and Martino, 2007).

The New Technology of Crime AFTER Work
- Internet Sex Crimes (sex tourism, child pornography, child predators/solicitation)
- Internet Hate Crimes
- Internet Stalking
- Cyber-Terrorism
- Spreading Viruses and Malicious Codes
- Hacking/Illegal Access to Data

The New Technology of Crime AS Work: Some Examples
- Internet Fraud Schemes: Nigerian letter, online auctions, drug/health frauds, lottery frauds, revictimization frauds
- Telemarketing Fraud Schemes: Investments, promotions, sales
- Identity Theft
- Credit Card/Check Fraud
- Phishing (for Profit)
- Internet Sex Crimes
- Sale of Private, Confidential, Personal Data
- Internet Piracy
- Theft of Computers, Computer Software, Internet Access
3. The New Technology of Criminal Justice

I examine five separate topic areas related to the application of new technological innovations, which—if successful—will lead to the prevention and control of criminal behavior: 1) crime prevention, 2) police, 3) courts, 4) institutional corrections, and 5) community corrections. In the following section, I examine the available research on the intended impact of innovations in each of these areas, focusing on a simple question: Is there sufficient evidence to support the continued use of these innovations? As I consider the scientific basis for each of these technological innovations, I have also attempted to identify the moral/ethical implications of various forms of technological innovations in criminal justice. As Marx (2008) has recently observed, we need to examine both the science and the ethics of new technology, recognizing that we have a choice—between the development and expansion of coercive technology and non-coercive crime prevention and crime control policies. Not surprisingly, the empirical foundation for new technological innovations has not been established; these innovations have not had their intended impact; they also have potential unintended consequences that are critical to keep in mind.

3a. The New Technology of Crime Prevention

Crime prevention is a concept that has been applied in a number of different ways to the problem of crime: it has been used to refer to both activities (such as crime prevention programs and/or strategies) and outcomes (such as lower levels of crime in communities and/or lower levels of offending/re-offending by individuals). In the name of crime prevention, researchers have examined the influence/role of formal social control mechanisms (e.g. the deterrent effects of police, courts, and corrections) and informal social control mechanisms (e.g. the influence—through mechanisms such as attachment, commitment, and involvement—of family, peers, school, work, community; the role of shame and belief systems/religion). In addition, crime prevention strategies have been targeted on different levels of prevention (primary, secondary, tertiary) and on the need for individual (i.e. private actions), parochial (group actions by neighborhood residents), and public actions (i.e. decisions to call the police) to prevent crime.

While crime prevention currently is used as a ubiquitous, catch-all phrase that can be applied to both criminal justice-based and non-criminal justice-based initiatives, my focus will be on strategies that utilize new technological innovations either to prevent crime (in particular places) or to prevent reoffending by targeted groups of offenders (sex offenders, mentally ill offenders) that do not rely exclusively on traditional actions by the police (arrest), courts (prosecution), and/or corrections (punishment, control, reform).

When considering the evidence of the impact of these strategies on crime, it is first necessary to define the term "crime prevention." I share Lawrence Sherman's view, which he presented in his influential report to Congress on What Works in the area of crime prevention (Sherman, et al., 1997:2):

Crime prevention is ... defined not by its intentions, but by its consequences. These consequences can be defined in at least two ways. One is by the number of criminal events; the other is by the number of criminal offenders (Hirschi, 1987). Some would also define it by the amount of harm prevented (Reiss and Roth, 1993:59-61) or by the number of victims harmed or harmed repeatedly (Farrell, 1995). In asking the Attorney General to report on the effectiveness of crime prevention efforts supported by the Justice Department's Office of Justice Programs, the U.S. Congress has embraced an even broader definition of crime prevention: reduction of risk factors for crime (such as gang membership) and increases in protective factors (such as completing high school)—concepts that a National Academy of Sciences report has labeled as "primary" prevention (Reiss and Roth, 1993:150). What all these definitions have in common is their focus on observed effects, and not the "hard" or "soft" content of a program.

According to a recent review of crime prevention technology by Brandon Welsh and David Farrington (2007:81),

Technological advances over the years have had a profound influence on the way we think about crime and the efforts that are taken to prevent it. Hard technologies to prevent crime cover a wide range of applications in different contexts, including metal detectors in schools, baggage screening at airports, bullet proof teller windows at banks, and security systems at homes and businesses.

There are other hard technology applications that quickly come to mind, including the use of personal protection devices (tasers, mace, lifeline/emergency call mechanisms) and ignition interlock systems with alcohol-sensor devices to prevent an individual from starting a car while intoxicated, and the various types of "social engineering strategies" described by Marx (such as target insulation, target devaluation, target removal, offender incapacitation, and offender exclusion) and advocates of crime prevention through situational crime control and/or environmental design manipulations (Marx, 2007; Clark, 1997).

While there are certainly a number of possible hard technology applications to crime prevention, Welsh and Farrington focus their research review exclusively on the only two hard technology innovations that they believe have known effects on crime: closed circuit television cameras (CCTV) and improved street lighting. To identify these crime prevention effects, the authors conducted a systematic review of the research on both forms of hard technology, which they have continually updated (Welsh and Farrington, 2002, 2004, 2006, 2007). Their findings are worth noting: "CCTV and improved lighting were more effective in reducing property crimes than in reducing violent crimes, with CCTV being significantly more effective than street lighting in reducing property crime" (2007:94). Of course, the majority of the evaluations reviewed by these authors focused on parking lots and/or garages; we simply do not have adequate empirical research to know whether these crime prevention effects will be found in other public places.

One additional caveat is in order when considering these findings. Both CCTV and improved street lighting strategies were found to be "far more effective in reducing crime in the U.K. than in the U.S." (Welsh and Farrington, 2007:95). The obvious question is: why? The authors consider a number of possibilities for this differential effect, including length of follow-up (shorter follow-ups show better results), the actual date the study was conducted and the specific technology used (newer studies/technologies do better), whether the strategy was implemented as a stand-alone innovation or used in conjunction with another initiative (stand-alones do worse), and cultural context/public support.
advances in computer protection technology, new anti-theft/target devaluation technologies, and social policy measures designed to ameliorate the environmental, economic, and psychosocial factors that encourage violent crime (Harris and Lurigio, 2007:103).

Harris and Lurigio provide a detailed review of the research on the design, implementation, and evaluation of the new generation of risk assessment and threat assessment instruments currently being used in this country and abroad. They focus their review of risk assessment on two offender groups: sex offenders and mentally ill offenders. For each offender group they identify new risk assessment technology (e.g. RRASOR, Static-99, SORAG, MnSOST; SONAR, SVR-20 for sex offenders; VRAG, Hare Psychopathy Checklist-Revised, HCR-20, ITC, COVR for the mentally ill) and then examine the available evidence of its effectiveness. The authors point out that one of the major paradoxes related to the development and expansion of risk-assessment technology in the area of violence prevention is that practitioners seem obsessed by the need to assess risk in groups of individuals (such as sex offenders) with very low failure rates (Harris and Lurigio, 2007). For some offender groups, risk appears much less important than stakes; for sex offenders in particular, it appears that the possibility of re-offending is more important than the probability of re-offending (Byrne, forthcoming).

In addition to their examination of risk assessment technology, Harris and Lurigio (2007) examined the development of new threat assessment protocols, and observe the following:

threat assessment...involves instruments or protocols to prevent violent incidents that rarely occur (e.g. an individual's risk of being a murder victim in a school shooting is less than one in a million), but nonetheless create great fear and anxiety in the general population, such as terrorism and violence in the school and workplace. The purpose of threat assessment strategies is to prevent events of targeted violence (e.g. at schools and in the workplace) in which assessing a particular individual's inherent risk of violence is secondary to the trajectory of behaviors leading up to the planned attack (Harris & Lurigio, 2007 pp. 104).

Harris and Lurigio's review revealed that threat assessment is only in its early stages of development and that the risk assessment field has a much sounder empirical base. However, it is critical to emphasize that we are not currently able to accurately predict either violent behavior or the likely location of violent acts.

Both risk assessment and threat assessment represent examples of how soft technology innovations can be applied to the prevention of crime by targeted individuals (sex offenders, mentally ill) or at targeted places (schools, workplace, airports). The problem is that whether we "profile" high-risk people or high-risk places, we simply do not have the necessary information to make accurate predictions; as a result, false positives are subject to unnecessary—and potentially harmful—surveillance and control. In our quest to prevent a small number of high stakes, but low-risk, crimes (e.g. school shootings, terrorist attacks, sex offending), we have essentially traded personal freedom for the (false) promise of crime prevention. To the extent that the actuarial assumption inherent in the newest generation of risk prediction devices results in the identification of minority group members as the potential "at-risk" group, the use of these risk instruments may institutionalize disparities by race and class (Gandy, 2007).

Perhaps equally important is the notion that we are wasting crime prevention resources on unproven strategies, many of them coercive in nature; a more prudent course would be to reallocate resources to non-coercive strategies with known crime/violence prevention effects (such as education, jobs, and poverty reduction) and fewer ethical concerns (Byrne & Roberts, 2007; Stemen, 2007).

3b. The New Technology of Policing

Changes in both the hard and soft technology of policing appear to be transforming local, state, and federal policing departments in a number of fundamental ways, but some scholars have raised questions about how much has really changed (Manning, 2003). Two recent reviews (Hummer, 2007; Harris, 2007) of technology and the police describe this transformation process, review the evidence of its impact on police practices and outcomes, and discuss the implications of technological changes in policing for the public. Both Hummer (2007) and Harris (2007) reach similar conclusions: police technology has not been found to significantly improve police performance. Similar assessments of the limited measurable impact of police technology on police performance have been reached by others who have reviewed the
available research on the impact of recent technological innovations on police performance (NRC, 2006; Manning, 2003).

Hummer (2007) recently identified several recent advances in the hard technology of policing, including: 1) non-lethal weaponry (chemical irritants, electric shock immobilizing technology, rubber, plastic, wooden bullet guns, beanbag shotguns, stove and acoustical weaponry), 2) various non-electric immobilizing devices (water pressure, trap nets, sticky foam), 3) technology to reduce the number of vehicular pursuits (barrier strips, vehicle disabling and tracking devices), and 4) technology designed for officer safety (improved bullet-proof vests, new body armor technology, improved patrol car protection technology). While there are certainly other hard technology applications in policing that can be identified (including new gunshot location devices, cameras to detect speeders and red light violations, the use of biometrics/improved fingerprint identification, and the hands-free communications systems being tested in patrol cars), Hummer has focused his review on a critical policing issue: how can we develop new technology that provides both officer safety and citizen safety and protection?

At the outset of his review, Hummer considers the argument that advances in new, hard technology are the inevitable consequence of the militarization of domestic law enforcement (Kraska, 2001). He observes that "While some of these devices were created exclusively for law enforcement use (Silberman, 2005), many of these technological advances originated from the U.S. military, NASA, DARPA (the Defense Advanced Research Projects Agency), other national research laboratories, and private sector corporations (Alexander, 2005; Hubbs and Klinger, 2004; Nunn, 2001)" (Hummer, 2007:133). I will return to this issue in the concluding section of my review, but it is important to keep in mind the profit factor: hard-technology police innovations are the direct result of the private sector's need to find lucrative, non-military (post-war) applications for military hard technology.

Focusing on the issue of officer safety, Hummer concludes that "While there are many factors in a complex dynamic associated with the significant decline in officer deaths over the past thirty years (Batton and Wilson, 2006), it seems reasonable to state that these innovations have played more than a negligible role" (2007:146). Apart from significant improvements in officer safety linked (generally) to advances in body armor, Hummer argues that there is little empirical evidence available to assess the impact of the other hard technology innovations on police performance. My own view is that while hard technology may account for significant improvements in officer safety, a more likely explanation is that these improvements in officer safety are linked to a general reduction in violence across the country over the past several decades.

In the conclusion of Hummer's review, he emphasizes the need for a "best practices," evidence-based review of the available research on these hard technology innovations. Given the cost of acquiring and maintaining these new hard technologies, it certainly appears that such a review is needed. Consider tasers, for example: there is no evidence that the introduction of this form of non-lethal technology has resulted in fewer instances where police will decide to draw and use their weapons; it appears that tasers and other non-lethal weaponry are actually being used to control individuals who would not—in the past—have been viewed as a threat necessitating a weapon-based response. It is in this context that it can be argued that we have "widened the net" of coercive police control, not only with the introduction of non-lethal force, but with a variety of other hard-technology applications. Given the fact that there is no evidence that spending money on the types of hard technology innovations improves police performance, one has to ask: why are we so enamored of these innovations?

There have also been a number of recent reviews of the design, implementation, and impact of soft information technology in the policing area (Pattavina, 2005; Manning, 2006; National Research Council, 2006). I will highlight the recent review by Christopher Harris (2007), who examined the impact of recent advances in information technology on police practices and performance, but I should emphasize that Manning (2003) and NRC (2005) cover the same ground and reach similar conclusions. Harris's review includes a description of new, technology-driven advances in 1) data collection and management (new record management systems, mobile data terminals, computer-aided dispatch (CAD) systems, information sharing via the internet), and 2) new data-driven police strategies (including Compstat, the use of computerized crime analysis and crime mapping software, and early warning/early intervention systems targeting police misconduct). Harris also examines the technological and organizational challenges to the full development of IT (information technology) in local, state, and federal police departments in this country.

Given the current debate over the effectiveness of both problem-oriented policing and community-oriented policing strategies (Skogan and Frydl, 2004; Rosenfeld, Fornango, and Baumer, 2005; Berk, 2005; Manning, 2003; Weisburd, Mastrofski, Greenspan, and Willis, 2003), Harris is cautious in his appraisal of the long-term impact of the IT revolution on police organization and administration. He concludes his review by placing these recent soft technology enhancements in their proper historical context:

While IT has the potential to enhance police work, and perhaps fundamentally alter traditional police practices, there is little evidence that IT has revolutionized policing when compared to the earlier eras of policing and the adoption of the telephone, two-way radio, and automobile. To the extent that newer IT has contributed to policing, it appears to have largely enhanced traditional practices (Harris, 2007:181).

Critics of the technological revolution in policing argue that we are "transforming policing" not by linking science to practice (Manning, 2008; Marx, 2008), but rather by developing strategies that utilize science/technology as a means to an end (coercive social control). Of course if such control-based technologies improved police performance, then such innovations would be on firm scientific ground, despite the obvious ethical/moral issues. In this regard, observe that clearance rates for every major crime category have dropped significantly over the past 50 years. For example, consider the crime of homicide: clearance rates have dropped from 92 percent in the late 60s to about 60 percent in 2007 (FBI, 2007). I would be hard pressed to offer an assessment of the positive effect of new technological innovations during this period, given these data on police performance.

3c. The New Technology of Law and the Courts

As federal and state lawmakers in states across the country scramble to write and rewrite laws defining the elements of—and punishments for—a wide range of technology-related crimes (among them distribution of steroids, creation of meth labs, 911 abuse,
new forms of financial and internet fraud, sale/distribution of child pornography on the internet, sex predators on the internet, human trafficking on the internet, identity theft, credit card fraud, theft of private information and trade secrets, and disruption of computer systems), court administrators in these same jurisdictions are considering exactly how to integrate cutting edge technologies—some used by the new categories of techno-criminals we have just created—into the traditional court process. The courts also play a role in sanctioning the use of (often coercive) control technology in policing (wiretaps, surveillance), prisons (race-driven classification schemes in California v. Johnson, use of segregation, and supermax), and community corrections (lifetime supervision laws and location restrictions for sex offenders, mandatory drug testing and treatment, etc.).

The courts appear to lag behind the police in their utilization of both hard and soft technology to improve the efficiency and effectivenes of the court process while also protecting the rights of defendants, victims, witnesses, and the general public (Cornell, 2001). In addition, the courts appear to lag behind the police in their use of new technology to improve staff and courthouse safety. According to a recent review by the Joint Technology Committee of the Council of State Court Administrators and the National Association of Court Managers, “Despite the billions invested on court technology, any objective observer would have to conclude that the courts have not received the return they should have from the time, efforts, and dollars spent on court technology” (Cornell, 2001: 17, as quoted in Corbett, 2007:225).

Absent an evidence-based review of the impact of technological innovations in court settings, policy-makers are often forced to make critical decisions regarding new technology initiatives based only on anecdotal assessments and case studies by court managers, which may or may not be accurate (Center for Court Innovation, 2007). There is a paucity of quality research on the impact on court technology and on court performance; the need for more—and better quality—research in this area is obvious.

Bellone (2007) recently described the application of a wide range of new technological innovations in courtroom settings across the country (CD-ROM, desktop and laptop computers, the internet, real-time transcription, video monitors and cameras, video conferencing, stored video/digital testimony, language translation devices, Braille systems and enhanced hearing devices, and the use of virtual reality simulations). He goes on to describe the rise of the cyber court (for instance, the Courtroom 21 Project at William and Mary School of Law) and then discusses the application of this new technology at key decision points in the court process, including 1) pretrial preparation, 2) the courtroom, 3) multi-jurisdictional and multi-court hearings, and 4) jury deliberations. In addition, he describes the use of new forms of hard technology (new weapons detection devices, shackles/restraints, video surveillance of the courthouse, and duress alarms) to improve the overall safety of courts. Finally, Bellone highlights the unique hard technology needs of one type of specialized court, the drug court (e.g. new drug testing technology, new integrated data systems).

Applying the evidence-based review criteria used by Sherman and colleagues (1997) to the topic of hard technology and the courts is revealing: we simply do not know “what works” in this area, because the necessary, independent quality evaluation research has not yet been conducted. Further clouding the picture is the cost of new technology and the likelihood that there will be differences in both access to technology and access to training on its use in the court process between public defenders and private attorneys; these differences in access and knowledge may affect outcomes in individual cases. After considering these issues, Bellone offers the following assessment: “Given the special significance of the courts, perhaps the slow pace of hard technological integration is appropriate and leaves room for social scientists and legal scholars to properly measure the impact—and ramifications—of such changes on the judiciary as a branch of government” (Bellone, 2007:207). My own assessment is more direct: one unintended consequence of technological innovation in the courts is that the documented disparity between rich and poor defendants (Taxman, Byrne, and Patavina, 2005) will likely increase.

Ronald Corbett (2007:211), the Executive Director of Massachusetts Supreme Judicial Court, begins his review of soft technology in the courts by noting that in 2002, “over 500 million dollars was spent by courts nationally on technology (Collins, et al., 2002).” Unfortunately, it appears that much of this funding did not have its intended effect, because one third of all IT projects are cancelled before completion; only a fraction of IT projects are completed on time and under budget; and even when completed, most IT projects cost nearly twice as much as initially projected (Clark et al., 2001). Clearly, Corbett raises the cost and implementation issues at the outset of his review for a reason: “In the midst of all the manifest commitment to technology and the related techno-boosterism sweeping through the professional organizations, a clear note of caution and some restraint on the rhetoric is justified” (Corbett, 2007:225).

Corbett has identified a number of specific soft technology innovations that have been implemented in courtrooms throughout the country, including: 1) the new generation of automated court record systems, 2) court-specific web site development, 3) online access to case information, 4) electronic court documents, 5) new software-supported case management and court performance measurement systems (such as CourTools), 6) RFID (Radio Frequency Identification) technology, 7) data warehouses such as Pennsylvania’s Justice Network, JNET, and 8) the emergence of problem-solving courts with new soft technology requirements (e.g. drug testing, sentencing support tools). After reviewing recent developments in each of these areas, Corbett highlighted a critical issue that is now being played out in court systems (and in court cases) around the country: How do we balance the public’s right to know with an individual’s right to privacy?

Our answer to this question will likely determine the future course of technological innovations in the courts. As Corbett correctly observes, “The most likely future for the clash between public access and individual rights to privacy is contained in this National Center For State Courts (2005:58) prediction: The battle between institutional efforts to protect the personal information of their clientele and the ingenuity of those who seek the sensitive data for dishonest endeavors will continue to escalate” (Corbett, 2007:225). This certainly highlights the “varied consequences” theme that runs through my review. Advances in soft technology—while perhaps improving court efficiency (we don’t know yet)—may further erode individual privacy rights. Since court data are being managed in many jurisdictions by private, for-profit companies, there certainly appears to be a link between the privatization of these functions and the erosion of personal privacy. The role of the private sector in the management of court records may need to be reexamined if individual privacy rights are a priority (Rebovich & Marino, 2007).
Our institutional corrections system has become the testing ground for a large number of hard technology and soft technology innovations, in part through the efforts of the Office of Law Enforcement Technology Commercialization, which attempts to utilize the expertise and resources in the private sector to address problems (e.g., the detection of cell phones in prisons, safe toilet seats, and other common items that can be turned into weapons) facing managers in the public sector (Barte, 2006). According to a recent review by the National Commission on Safety and Abuse in America's Prisons, we spent sixty billion dollars on corrections nationwide last year alone; the vast majority of these funds were used to build prisons and to house and manage prisoners (Gibbons and Katzenbach, 2006). While reliable estimates on the proportion of total corrections spending targeted for new technology development are not available, it seems safe to assert that it is a substantial sum.

Given the sheer number of prisons (1,668 in 2000) and jails (3,376 in 2000), and the amount of money our nation appears willing to spend to incarcerate offenders, it is not surprising that private-for-profit companies would be interested in public/private partnerships generally, and the development and testing of new technologies in particular. However, questions need to be answered about the impact of corrections technologies on the behavior, mental health, and physical health of offenders, both during their time in prison and upon return to the community. In the United States, inmate-line officer ratios are generally reported to be between 3:1 and 8:1 (Sourcebook, 2005), but reports of much higher ratios (100:1) are not unusual; by comparison, the ratios found in British prisons are much lower, allowing for closer interaction between staff and inmates and different strategies for staff management and offender change (Byrne, Hummer, and Taxman, 2008).

We rely on the technology of control in this country because we have no reasonable alternative, given our decision to use prison as the sanction of choice for certain categories of offenders (particularly drug offenders). In fact, we have made a conscious choice to imprison a large number of people (over 2 million at last count) and to supervise them using a relatively small number of line staff (270,317 custody/security staff in 2000, according to the Sourcebook of Criminal Justice Statistics, 2003: 96). While there is a continuing debate on the general deterrence-based, crime reduction effects of a prison sentence (Webster, Doob, and Zimring, 2006; Cook, 2006; Levitt, 2006), there appears to be an emerging consensus that 1) prisons are dangerous places, 2) what happens in prison doesn't stay in prison, and 3) offender change—not offender control—should be the primary mission of institutional corrections (Byrne, Hummer, and Taxman, 2008). It is in this broader context of sentencing policy and correctional philosophy that we now consider the new technology of prison control.

A recent review by Jacob Stowell (2007) highlighted the application of new, hard technology in three general areas of institutional control: 1) facility monitoring (e.g. weapon and contraband detection, remote monitoring of inmates, officer duress systems, and perimeter security), 2) inmate/officer interactions (e.g. language translation devices, less-than-lethal force), and 3) high-risk inmate control (e.g. the use of supermax prisons). According to Stowell (2007:242), "With the size of the incarceration population increasing and jail and prison budgets shrinking, the ability to effectively manage prisoners has never been more difficult. One challenge that the field faces is how to strike a balance between the amount of resources dedicated to inmate control (technology upgrades) compared to that devoted to treatment (i.e. mental health services, programming) of inmates." The recently expanded role of the private sector in the construction and management of prisons is another potentially problematic area (Herival and Wright, 2007), because it seems safe to assume that the public and private sectors may have very different views of how to define success.

Byrne and Pattavina (2007) completed a recent review of soft technology applications in institutional corrections that argued for further research on the appropriate "tipping point" between strategies designed to control offenders and strategies designed to change their attitudes, values, and behaviors. The authors identify a variety of current and potential soft technology applications to problem solving in institutional settings, focusing on a wide range of inmate classification, treatment and control and staff (management and protection) activities, including: 1) new techniques for the initial classification of inmates and subsequent offender location decisions; 2) new offender monitoring strategies (both health and behavior related); 3) crime analysis, hot-spot identification, and problem-oriented conflict resolution strategies within prison and jail; 4) information-sharing with police, courts, corrections, public health, and public/private sector treatment providers; 5) the application of crmne mapping and neighborhood risk assessment in reentry initiatives and 6) performance measurement system development in prisons and jails.

At the conclusion of their review, Byrne and Pattavina (2007) offer an alternative perspective on soft technology applications, suggesting that various forms of information technology—in particular, prison classification at the outset of an offender's prison experience and reclassification nearing the end of an offender's time in prison as he/she prepares for reentry—can be revised to emphasize the goal of offender change rather than short-term offender control. The results of a recent evidence-based review of the research on prison violence and disorder by Byrne, Hummer, and Taxman (2008) support this position:

Given recent reviews highlighting the over-classification of female inmates (Austin, 2003), and the expansion of protective custody, administrative and disciplinary segregation (Commission on Safety and Abuse in America's Prisons, 2006), it appears that the primary purpose of current external and internal classification systems is the short-term control of our inmate population. There is no evidence that our current emphasis on control-based classification systems makes prisons any safer; but there is a mounting body of evidence that we can reduce violence and disorder in prison by increasing inmate program participation rates.

Byrne and Pattavina (2007) offer a framework for changing offenders while in prison by linking offender assessment to offender placement in various forms of prison treatment (for mental health problems, substance abuse problems, educational deficits, employment/skill deficits, etc.). As Gilligan and others have pointed out (Gilligan and Lee, 2004), one of the ironies of imprisonment is that some of the most compelling evidence of offender change is from evaluations of programs operated in institutional settings (e.g. prison therapeutic communities and cognitive restructuring programs located in both prisons and halfway houses). Similarly,
Liebling (2004) and others have argued that prisons can and should be monitored and judged in terms of their “moral performance” (e.g. staff-inmate interactions, procedural justice, access to treatment, etc.), based on a simple axiom: The moral performance of prisons will affect the moral performance of prisoners, while in prison and upon release to the community (Byrne, Hummer, and Taxman, 2008). The U.S. prison system has demonstrated that it is possible to design and operate a prison system from which few prisoners can escape (Byrne and Hummer, 2007). However, over 90 percent of these prisoners will return to the community; what we gain in coercive short-term offender control is essentially lost when these offenders “fail” in the community.

3e. The New Technology of Community Corrections

The growth of our corrections system has not been limited to institutional corrections. Community corrections populations have actually grown at a faster pace than the populations of its institutional counterpart, but what has shrunk over the past decade and a half is the proportion of corrections spending allocated to community corrections. (For example, last year, community corrections supervised 70 percent of the total corrections population but received about 20 percent of all corrections funding.) According to a recent Bureau of Justice Statistics Bulletin, *Probation and Parole in the United States, 2004*, authored by Lauren Glaze and Seri Palla (2005: 2), “The number of adult men and women in the United States who were being supervised on probation and parole at the end of 2004 reached a new high of 4,916,480, up from 3,757,282 on December 31, 1995...Overall, the correctional population increased by nearly 2.5 million, or 57 percent, from 1990 to 2004. Probationers accounted for 51 percent of the growth (or 1,262,000), followed by prisoners (27 percent or 679,000), jail inmates (12 percent or 309,000), and parolees (9 percent or 234,000).” The reason these numbers matter is that as the scale of the community corrections system has increased, community corrections managers have embraced a wide range of hard and soft technologies designed to improve the community control of offenders without adding significant numbers of new personnel.

There are a variety of ways that community corrections managers can apply new technological innovations to the management of offenders under community supervision. For example, one strategy would be to use the results of risk classification to identify a group of low-risk offenders that do not need direct supervision. In 2004, 26 percent of all probationers were not placed on active supervision, up from 21 percent in 1995; the comparable numbers for parole move in the opposite direction, with 15 percent of parolees not placed under active supervision, down from 22 percent in 1995 (Glaze and Palla, 2005). When fiscal resources are scarce, the size (or threshold) of the low-risk population targeted for non-supervision can be increased with little or no effect on public safety (Austin, 2006).

For the remaining offenders on active supervision, one hard-technology option involves the use of electronic monitoring, and this monitoring function is quickly moving to the private sector (see Harris and Byrne, 2007). Active offender supervision using new technology innovations will likely vary by the seriousness of the conviction offense. According to Glaze and Palla (2005:6), “The largest percentage of the probation population was convicted of a drug law violation (26 percent), followed by a DWI (15 percent) and larceny/theft (12 percent).” By comparison, parolees (in 2004) have typically served at least a year—often much longer—in prison for one of the following crimes: violent (24 percent), property (26 percent), drug (38 percent), and other (12 percent) crimes.

For both parolees and probationers, success rates have remained stable for the past decade: about 60 percent of all probationers and about 46 percent of all parolees “successfully met the conditions of their supervision” (Glaze and Palla, 2005:9). However, most observers feel that these success rates are unacceptably low, especially when viewed in terms of long-term declines beginning in the early eighties, a period in community corrections history marked by a new community corrections organization, its technology in the classification, treatment, and control of offenders: 1) the new generation of classification instruments used in community corrections (LSI-R, PCL-R, HCR-20, VRAG, LCSR, RRASOR, Static-99, MnsOST-R, and SVR-20), 2) new approaches to offender treatment based on the Risk/Need Responsivity model (and using the COMPAS classification system), 3) new case management information technology (e.g. the SMART, Supervision and Management Automated Record Tracking, system), and 4) new approaches to information sharing, crime
mapping, and the assessment of community risk level for offenders under community supervision (and during reentry). Unfortunately, the necessary evaluation research on the implementation and impact of these soft technology innovations has not been completed, leading Pattavina and Taxman to conclude that we do not know whether improvements in information technology have resulted in the improved performance of the community corrections system.

One final caveat appears appropriate. Given the expanding role of the private sector in community corrections, it makes sense to ask a simple question: If we contract electronic monitoring/supervision to one vendor, assessment to a second vendor, and service provision/treatment to a third vendor, then what is left for line community corrections officers to do? This is a question that will need to be addressed; and how it is resolved will determine whether privatization is just a short-term “fad” or a long-term strategic reduction in reliance on public social control mechanisms.

4. Innovations in Criminal Justice Technology: Issues to Consider

Any new technological innovation is likely to have both intended and unintended consequences for crime and social control that are important to understand. Nonetheless, three critical issues come immediately to mind. First, perhaps the most salient issue related to the new technological innovations is whether—over time—we will replace people (police officers, court officers, judges, corrections officers, and community corrections officers) with various forms of thing technology (CCTV, cameras that detect speeders, wired courts, electronic monitoring, supermax prisons, etc.). For example, why do we need police officers patrolling the streets (and highways) when we have the technological resources (via cameras to detect speeders and red light violations, and CCTV to monitor public places) to remotely monitor activities and deploy a smaller number of police to address crime problems that are detected? The downsizing of police force manpower may be an inevitable consequence of this type of technological innovation, which is one reason that technological change may be viewed suspiciously by line personnel and the unions that represent their interests. Similar scenarios can be offered about the likely impact of various technological innovations in the courts (electronic filings, sentencing software) institutional corrections (the techno-prison, new identification and prisoner tracking devices), and community corrections (electronic monitoring with real-time tracking/location restrictions). What do we lose when we rely on technology rather than people to perform essential criminal justice tasks? My guess is that Gary Marx’s admonition—written about electronic monitoring over 20 years ago—is right on target: there is no soul in the new machine.

Another aspect of the person vs. thing technology analogy is worth considering here. It is certainly possible that our increased reliance on technology will lead us further down a potentially treacherous road: an increased reliance on both coercive surveillance and coercive control strategies. For those who draw parallels between domestic policing and military strategy (e.g. Kraska, 2001), it may be helpful to consider a recent shift in the approach of the military to the question of troop strength/deployment strategy: we are now considering reducing our reliance on large, standing forces of military personnel (e.g. in June, 2008, there were 150,000 troops in Iraq) and instead creating a number of small, highly trained, and technology-rich quick-strike Ranger-style units that can move to (and from) various “hot spot” areas as needed. This strategy may represent a possible deployment model for local, state, and federal police agencies that use various forms of hard technology (e.g. cameras, gunshot location devices, CCTV) and soft technology (e.g. crime mapping, hot spot analysis) to monitor areas (and analyze crime patterns) from a central location.

While it is certainly possible that such strategies may increase police performance initially, the longer-term effects may not be so positive, due to the distrust of the police in high-crime, poverty-pocket areas that will likely be fostered by such strategies. Before we move too far in this direction, I think we need to consider the alternative: the development of non-coercive crime prevention and crime control strategies (Cole and Lobel, 2007). We can spend money on the latest unproven technological innovation in our search for an effective crime prevention and/or crime control strategy, but it is worth considering whether similar—or greater—crime prevention/control effects can be realized by using this money on proven strategies to improve drug treatment and education systems, create job training programs, improve housing, relocate families living in high-crime areas, reduce poverty, or hire more police to walk, talk, and problem solve in these “at risk” communities (Stemen, 2007; Byrne and Roberts, 2007).

A second related issue is whether our fascination with the new technology of offender control will result in the continued development and expansion of criminal justice policies that minimize the possibility—and undermine the prospects—for individual (offender) and community change (Byrne and Taxman, 2006). One doesn’t have to look any further than our recent prison build-up to find a good example of how our reliance on offender control in institutional settings—we spent 60 billion on corrections last year alone, with over three quarters of that total allotted to prison management—has undermined our ability to provide treatment to offenders (for substance abuse, mental health, education/skill deficits) that might actually change their (criminal) behavior, both while in prison and upon reentry to the community (Gibbons and Katzenbach, National Commission on Safety and Abuse in American Prisons, 2006). To the extent that new technological innovations reinforce what David Garland has aptly labeled a culture of control, technology may be moving our corrections system in the wrong direction. Perhaps we need to think in terms of a correctional paradigm that emphasizes the new technology of offender change and would represent a departure from our current emphasis on control technologies; in doing so, we would recognize a simple lesson of history: more often than not, “brute force” fails (Kleiman, 2005).

And finally, out of necessity rather than by design, we certainly need to consider the long-term consequences of privatization of key criminal justice system functions, including information management, offender/place-based monitoring, and offender control. In large part because the line staff and management in most criminal justice agencies do not currently have the necessary technology-based skill sets, we are forced to rely on the private sector today more than at any point in our history, particularly in the area of information technology. It is certainly possible to envision a Brave New World of crime prevention and control, where the private sector’s helping, short-term support role (e.g. in the areas of information technology, system integration, electronic monitoring, and private prison construction/management) expands to the point where private sector crime con-
The New Technology of Criminal Justice: Intended vs. Unintended Consequences

<table>
<thead>
<tr>
<th></th>
<th>Intended</th>
<th>Unintended</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Crime Prevention</strong></td>
<td>Prevent Crime</td>
<td>Less Freedom</td>
</tr>
<tr>
<td></td>
<td>Less Crime</td>
<td>More Distrust</td>
</tr>
<tr>
<td></td>
<td>Increased Officer Safety</td>
<td>More Coercion</td>
</tr>
<tr>
<td></td>
<td>Less Harm to Public</td>
<td>Increased Harm</td>
</tr>
<tr>
<td><strong>Police</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Courts</strong></td>
<td>More Efficiency</td>
<td>More Disparity</td>
</tr>
<tr>
<td></td>
<td>Better Decisions</td>
<td>Less Privacy</td>
</tr>
<tr>
<td><strong>Institutional Corrections</strong></td>
<td>More Control</td>
<td>Less Change</td>
</tr>
<tr>
<td><strong>Community Corrections</strong></td>
<td>More Control</td>
<td>Less Change</td>
</tr>
</tbody>
</table>

trol ultimately replaces public sector crime control in several critical areas (crime prevention, offender monitoring, place-based monitoring, and various forms of offender control). If this occurs, my concern would be that the moral performance of the criminal justice system will suffer, because a concern for the economic bottom line will have negative consequences in a number of critical areas (privacy protections, resource availability and quality, fairness, procedural justice).

Conclusion: Understanding the Context and Consequences of Technological Change

It should be apparent from my brief, selected review of the available research that technological innovation will likely have both intended and unintended consequences for criminal justice organizations—and, by extension, the public—that are important to consider. Given the weak empirical foundation for these innovations (the science is not convincing) and the potentially detrimental side effects (the ethics are questionable), it seems reasonable to ask: Why change? We are currently experiencing a long-term downward trend in crime, with violent crime rates down over twenty percent since 1995 and our overall crime rate back to where it was in 1970.

The pressure to innovate is not related to a deteriorating crime problem; in fact, the opposite is true. However, it could certainly be argued that the need to innovate comes from a source more directly linked to criminal justice strategic planning and decision making: the poor performance of the criminal justice system in several key areas. For example, police clearance rates for homicide have dropped from over 90 percent in the late 1960s to 60 percent today, with similar precipitous drops for other categories of violent crime. The court system has developed a variety of reforms designed to address the long-standing problems of race and class bias over the past two decades, including the introduction of actuarial-based pretrial and sentencing decision-making tools (e.g., sentencing guidelines), but these reforms appear to have simply institutionalized race- and class-based disparity; the problem still remains. The institutional correctional system has been criticized in a number of performance-related areas in a recent comprehensive review by the National Commission on Safety and Abuse in America’s Prisons. While there is an ongoing debate on the extent of the violence problem in prison, there is an emerging consensus that our prison system “makes offenders worse” in critical areas, such as mental health and physical health. Offenders leaving prison and being supervised in the community are failing at a much higher rate today than in 1980, with parole success rates dropping from 60 to 40 percent and probation success rates dropping from 80 to 60 percent.

Assuming that it is the poor performance of the criminal justice system that drives our current fascination with a wide range of technological innovations, the next logical question after “Why change?” is: “Why have we decided to move toward these forms of technology?” The short answer is that we appear to favor innovations that increase our ability to control, rather than change, individuals. Gary Marx’s perspective on the use and misuse of technology in support of social control challenges much of the current thinking about the benefits of technological change.

The study of social control is a central element of sociological understanding. By social control I refer to the multi-faceted study of norms and rule enforcement. This can involve studying the creation of norms, processes of adjudication and sanctioning and also the broad societal guidance, integration and ordering which were of concern to early theorists of industrialization and urbanization.

Social control also centrally involves efforts to enforce norms. ... An important part of contemporary enforcement efforts involves using science and technology to strategically structure normative environments so that rule breaking is reduced and the identification of offenders and offenses and the minimization of harm are increased.

I am particularly interested in engineering efforts as applied to settings where there is a conflict of interest between agents and subjects of social control. While all technological control efforts have elements in common, those involving dissensus show some distinctive characteristics such as the dynamics of control and counter-control and the centrality of human rights issues (Marx, 2007 pp. 347).

I think it is fitting to conclude my review with another quote from Marx, which I believe highlights a critical insight: We need to find ways to apply new technology to the problems related to the monitoring and control of individuals and places; but we also need to find ways to use technology for an even more important purpose—to reinforce moral performance at both the institutional and individual level.

As Marx (2007) wryly observed, a well known, if often naive expression (given that individuals and groups do not start with equivalent resources), holds that where there is a will there is a way. This speaks to the role of human effort in obtaining goals. With the control possibilities made available by science and technology this may be reversed to where there is a way there is a will. As the myth of Frankenstein implies, we must be ever vigilant to be sure that we control the technology rather than the reverse. As Jacques Ellul (1964) argues there is a danger of self-amplifying technical means silently coming to determine the ends or even becoming ends in themselves, divorced from a vision of, and the continual search for, the good society. (Marx, 2007).
I think we need to continue to evaluate the effectiveness of new control-oriented technology in institutional and community corrections, documenting both the intended and unintended consequences of these types of technological innovation. However, we also need to recognize that new technology does not have to be synonymous with offender control. By investing in a wide range of (hard and soft) offender change technology (e.g. new treatment-oriented prisons and jails, new treatment-oriented community corrections programs, new drugs to assist addicts and the mentally ill), we may be able to find ways to apply new technological innovations for an even more important correctional purpose—to change offenders in ways that will result in desistance from criminal behavior.

References


