



E-Government Strategies

TOOLS TO ENHANCE COMMUNITY POLICING

by Ari Schwartz and Cynthia Wong

INTRODUCTION

E-Government involves using information and communications technology (ICT) to enhance the relationship between the government and its constituents.¹ Developing “citizen-centric” models that involve stakeholders inside and out of government is the key to real e-Government reform. When effectively implemented, e-Government transforms existing processes by fostering transparency, eliminating distance and other divides, and empowering people to participate in the political processes that affect their lives.

E-Government projects present unique opportunities to strengthen community policing efforts. ICT tools for collaboration, discussion, and problem solving can enhance communication between neighborhoods and local police by providing new avenues to share information unconstrained by distance and time. In turn, increased information flow facilitates collaborative problem solving by helping police identify community issues, eliminating barriers to collective action, and leveraging untapped local capacity. As the following sections demonstrate, integrating e-Government projects as part of a larger, more traditional community policing strategy has the potential to provide a variety of benefits to both police and residents.

THREE PHASES OF E-GOVERNMENT²

E-Government is an evolutionary, multi-faceted process that we may view as consisting of a set of phases. One way of conceptualizing these phases is in three parts: publish, transact,

¹ E-Government may be conceptualized in many different ways. One report defines e-Government as “the use of ICT to promote more efficient and effective government, facilitate more accessible government services, allow greater public access to information, and make government more accountable to citizens.” The Working Group on E-Government in the Developing World, “Roadmap for E-Government in the Developing World,” (2001), 1, available at <http://www.pacificcouncil.org/pdfs/e-gov-paper.f.pdf>. Other groups focus on the potential of e-Government to strengthen civic engagement and other democratic goals. See, e.g., E-Democracy.Org, www.e-democracy.org (last accessed July 28, 2006).

² See the Center for Democracy and Technology, “The E-Government Handbook for Developing Countries,” (2002), 3–5, available at www.cdt.org/egov/handbook/2002-11-14egovhandbook.pdf. See also the Council for Excellence in Government, “e-Government: The Next American Revolution,” (2001), available at www.excelgov.org/admin/FormManager/filesuploading/bpnt4c.pdf.

and interact. Although interact and transact applications require more sophisticated back-end capabilities, some e-Government projects have components of more than one phase, and all three phases can be implemented simultaneously. This conceptual framework for understanding the process of e-Government development is applicable from the police beat all the way to the governance of federal programs.

Publish

Publish sites seek to disseminate information *about* government and information compiled *by* government to as wide an audience as possible. The quality of publish Web sites depends on the amount of content, the usefulness of the content, and how often content is updated. Web site quality also depends on factors such as navigability, usability, search capacity, accessibility, and download time. Even more advanced portal applications enable residents to personalize content based on their individual needs and interests. For example, community policing portals can publish crime data by neighborhood and link to other city service information that is of value to people in their daily lives. Such customizable portals would enhance the value of online community policing and encourage wider use because they support diverse segments of the community.

Local governments and police departments generate huge volumes of information, much of it potentially useful to individuals and businesses. The Internet and other advanced communications technologies can bring this information quickly and more directly to citizens. Publish implementations of e-Government diverge widely in their design and content, but governments at any level can generally start the process of e-Government by publishing government information online, beginning with rules and regulations, government documents, event calendars, and forms. Police departments can publish crime data, news alerts, safety tips, and information about penitentiary and parolee releases. Advanced publish features can also disseminate content to cell phones and PDAs.³ Finally, police departments can easily link community policing portals to other city departments that deal with related quality of life services (e.g., vehicle tow information or public housing rules).

Publish projects are often thought of as basic building blocks for larger e-Government programs, but the release of vital information to the community, even if only for the purpose of building transparency and mutual trust, can have a profound impact on stakeholder views of government.

Transact

A transact Web site offers a direct link to government services, available at any time. Perhaps the biggest incentive for city and police departments to use and provide ICT services is to streamline currently bureaucratic and labor-intensive procedures, which can save money and increase productivity in the long run. Successful transact projects target those services that

³ Many label this practice as mobile government or “m-Government.” For example, Japan offers m-Government services through its e-Government portal at www.e-gov.go.jp (accessed July 26, 2006). The National Policy Agency of Japan disseminates photos of wanted suspects through cell phones. The Hong Kong government is also developing a range of new m-Government initiatives. “E-Government in Hong Kong,” <http://www.info.gov.hk/digital21/e-gov/eng/init/mgov.htm> (accessed July 26, 2006).

residents have an immediate use for while also addressing the concerns of government workers whose role will change because of the innovation. In addition, officials should integrate transact initiatives with process reform by streamlining processes before launching them online.

Transact sites can enhance productivity by making processes that require government assistance or approval simpler, faster, and cheaper. For example, some police departments currently allow individual and business users to input and track neighborhood problems online. In turn, the police link this new functionality to the 311 system and other city services.⁴ Moreover, police departments could also allow users to submit routine incidence reports for “suspectless” crimes (e.g., bicycle theft or vandalism) directly through department Web sites.⁵ Local governments often consolidate these initiatives and create a portal for all transact services.

Interact

Interactive e-Government involves two-way communications. Governments use e-Participation projects to collect citizens’ and businesses’ views so constituent interests and needs are better represented in government programs and police initiatives. The goal is to increase the responsiveness of city departments to citizens and businesses based on those submissions. E-Participation starts with basic functions like providing e-mail contact information for government officials and police officers or simple feedback forms. Other tools include chat rooms, online surveys, electronic newsletters, and e-mail lists. Online community policing sites can provide tools for virtual beat meetings, web tip systems, neighborhood canvassing, social service agency referrals, neighborhood beat blogs, and feedback forms for police complaints or compliments. E-Participation applications may also have a publish feature, presenting relevant background information, decisions, and other materials to help citizens and businesses understand certain public policy or crime issues. These applications can then enable public comment on policymaking by breaking down complex policy issues. More advanced e-Participation functionality can include the ability of an individual to personalize Web pages or sites to meet one’s needs.

This phase of e-Government may also include the creation of citizen or government forums. Forums facilitate communication among individuals who, while living in the same neighborhood, may not otherwise interact because of time constraints or physical accessibility. E-Consultation takes the process one step further than e-Participation, facilitating online comment on a specific policy or police program while the issues are under active consideration by the government. For all projects, it is important that local officials show citizens that their engagement matters by informing them of the outcomes of their online comments.

⁴ Many cities already allow residents to submit requests for a variety of city services online. See, e.g., “311 At Your Service – City of Chicago,” https://servicerequest.cityofchicago.org/web_intake_chic/Controller (accessed July 28, 2006); “e-Services – Online Services – District of Columbia,” http://dc.gov/more_services.asp?tab=0&category=services (accessed July 28, 2006).

⁵ The San Francisco Police Department (SFPD) began receiving crime reports for minor offenses online in 2004. As of April 2006, the SFPD has seen both an increase in crime reporting and an increase in time available to officers to respond to emergency calls, conduct preventive patrols, and interact with the community. Beth Winegarner, “Police Say Online Crime Reporting Saves Officers Time,” *The Examiner*, April 17, 2006.

Finally, local governments may consider hosting independent, citizen-initiated forums and neighborhood e-mail lists by providing technical infrastructure and support while allowing communities themselves to create and manage content. To ensure that a diversity of voices are represented, governments and local police departments should promote the availability of the forums both on community policing Web sites and at neighborhood beat meetings. Reserving space solely for community use helps build trust by allowing communities to identify, frame, and clarify issues independent of city officials.⁶ Such forums constitute online communities where people can exchange ideas, broaden public awareness of issues, and establish new opportunities for activism constrained neither by time nor distance.

In the law enforcement context, increasing and enhancing communication between neighborhoods and local police strengthens civic engagement and contributes to building public trust in law enforcement. In turn, increased participation and community buy-in greatly boost the effectiveness of community policing efforts. However, it is important to note that interact projects are also the most likely to fail because a critical mass of participants is necessary to make them work.⁷ Local governments and police departments should engage citizens collaboratively in the design phase and be proactive about soliciting participation by promoting interact projects using traditional media.

TRANSFORMING GOVERNMENTS THROUGH E-GOVERNANCE

E-Government is about transforming the way government interacts with the governed. That process requires a coherent strategy, beginning with an examination of a community's political will, resources, regulatory environment, and the ability of the community to make use of planned technologies. There is no-one-size-fits-all strategy, but we have identified five essential elements in the transformation process.

Planning for Process Reform⁸

Successful e-Government is about the creation of new processes and new relationships between government and its constituents. Often, the business world launches new e-Commerce products and changes the administration and bureaucracy around the growth of the site. Government is rarely as flexible. E-Government initiatives are likely to have the wid-

⁶ See "Local Issues Forum Guidebook," E-Democracy.Org UK – Issues Forum 14–17, 52–57 (March 2005), available at <http://e-democracy.org/uk/guide.pdf>. E-Democracy recommends that creators of local issues forums maintain a political buffer between issues forum administrators and government bodies to lend greater legitimacy and transparency to the process. See also Keith Hampton and Barry Wellman, "Neighboring in Netville: How the Internet Supports Community and Social Capital in a Wired Suburb," *City & Community* 4, no. 2 (2003): 16–26, <http://www.asanet.org/galleries/default-file/HamptonWellmanCC.pdf> (accessed July 13, 2007).

⁷ E-Democracy emphasizes the importance of recruitment efforts to establish a critical mass of participants to sustain a discussion and prevent online ghost towns. Interview by Italian Polix.it with Steven Clift, E-Democracy (October 16, 2001), available at <http://www.mail-archive.com/do-wire@tc.umn.edu/msg00364.html>. See also "Neighboring in Netville," which examines one case study that found that a local e-mail forum enhanced neighborhood ties and facilitated discussion and mobilization around local issues. However, the case study also suggests that the ability of the network to provide new affordances for community ties depended on the network's "always-on" nature and universal access to the list.

⁸ Accenture considers process reform (or "service transformation") as the 4th phase of e-Government. Accenture characterizes this phase of e-Government as a period of wider integration and organizational changes across departments. The focus of e-Government shifts to wide scale improvements in Customer Relation Management. Accenture, "eGovernment Leadership: Engaging the Customer," (2003), 6–10, https://www.accenture.com/NR/rdonlyres/9988450E-C3A2-4094-875B-CA4F1E3F3696/0/engaging_customer.pdf.

est impact when pursued within the context of broader strategies for governmental reform, improved access to ICT, and community development. This revolutionary change takes advanced planning to bring success.

Leadership

To achieve the e-Government transformation, elected officials and administrators who understand the technology and the policy goals involved, and who will push for reform, are needed at all levels of government. Project champions must articulate a sense of purpose that can propel the e-Government initiative through all the necessary steps. As police departments and city agencies adopt new methods of collaboration and organization, this unifying theme will ensure the cooperation of disparate factions and the long-term commitment of resources and expertise. Project leaders can help ensure success if they elevate the public profile of their vision and press for its effective implementation by tying it to broader community goals. Many successful e-Government initiatives have been spearheaded by a dedicated office with high-level support.

Strategic Investment

Governments will need to prioritize programs to maximize available funds in view of tightly limited resources. This requires the formulation of concise objectives for each program and an explicit route to reach those objectives. Projects should have clear value in terms of enhancing transparency, increasing citizen participation in community policing, cutting bureaucratic red tape or saving money. Administrators must establish standards and benchmarks to measure the relative success of these projects.

Collaboration

City governments and police departments will have to explore new relationships among agencies and departments. Agencies may have to overcome traditional reluctance to work with each other to maximize benefits of scale in e-Government projects. In addition, police departments should develop partnerships with the private sector, community-based organizations, and residents to ensure quality and accessibility of community policing e-Government projects.

Civic Engagement

Community involvement and empowerment are key components of any successful community policing initiative. To develop a strong citizen- and community-focused vision, policy makers must keep the ordinary citizen and target community in mind when designing e-Government initiatives. Policy makers should encourage all stakeholders to participate in defining what their shared vision of e-Government should accomplish within a community policing program. Once leaders in government clearly define that vision, they must communicate it across all sectors, not just to those who will implement it.

CHALLENGES AND OPPORTUNITIES⁹

Once governments commit to strategies that will transform their governance processes, significant challenges and opportunities will often arise during their implementation. We have identified several considerations that policy makers must address in the design and implementation of any e-Government initiative:

- *Interoperability:* Rather than adding new systems on top of outmoded legacy systems, e-Government planners should develop systems and formats that work together and across departments.
- *Records management:* Governments have unique needs in the field of records management. New technologies are being created to help manage information and policy makers should take advantage of these new technologies accordingly.
- *Permanent availability:* Policy makers should design applications with preservation and documentation in mind while also taking into account issues of relevancy, usability, privacy, and security.
- *Education and marketing:* Education and outreach programs will be needed to ensure community and citizen participation. Policy makers should also conduct research to ensure that online services respond to actual needs and that the implementation suits the target audience.
- *Public/private competition/collaboration:* Policy makers should consider cooperative projects between the public and private sectors carefully. Public and private interests should work together as partners and not necessarily for political or economic gain. New partnerships and alliances can have unforeseen consequences, so it is important to review such relationships frequently to ensure that both parties are pleased with the arrangement.
- *Workforce issues:* Human resources must be structured and managed with e-Government goals in mind. Because ICT implementations of community policing initiatives require collaboration across city departments, civil servants and police officers need training and leadership to integrate themselves into the new information structure.
- *Cost structures:* While planning and budgeting in a changing climate is difficult, governments should seek to invest in sustainable programs that can produce savings. Policy makers should articulate functionalities and goals clearly to ensure that they are attainable with available resources.
- *Benchmarking:* Governments must regularly evaluate the progress and effectiveness of their e-Government investments to determine whether programs are meeting stated goals and objectives on schedule.
- *Public policy and law:* Policy makers implementing e-Government programs must consider the impact of existing law and public policy. This effort must incorporate a

⁹ See e-Government: The Next American Revolution at 6–16. See also E-Government Handbook at 11–22.

- review of current practices that encompasses more than just law and policy related to the use of technology. Old policies and overlapping authority can greatly complicate a project. Administrators may have to adopt new policy directives before collaborative online initiatives can function smoothly.
- *Digital divide, disability access, literacy and e-Literacy:* Even in areas where access to technological infrastructure is nearly ubiquitous, there are still marginalized groups who are unable to make use of ICTs. Programs must take special steps to include people who are not e-literate and to bridge the digital divide, including education and outreach to vulnerable groups who are traditionally isolated from technology. For example, policy makers should design online services with appropriate interfaces for people of all physical abilities.
 - *Privacy:* Privacy is one of the most important issues facing the Internet. Governments must be responsible custodians of the enormous amounts of personal information they hold. Government Web sites and online services must adhere to privacy best practices. Policy makers should integrate these practices during the planning and design phases of any e-Government initiative.
 - *Security:* Security must be addressed in the design phase because security breaches can shatter public trust in e-Government efforts. Without trust, citizens will not use online services that could potentially place their personal privacy or security at risk.
 - *Transparency:* Government and police department transparency should be embedded in the design of ICT systems. When citizens and communities do not understand how decisions are made, they are less likely to participate actively in problem-solving efforts.

CONCLUSION

The principles of e-Government can be applicable to online community policing efforts. The process of picking projects that are right for the community and developing them to transform the way that stakeholders interact with government is becoming a more established process. In particular, engaging stakeholders throughout this effort will be essential for local law enforcement to develop projects that truly improve the community and their interactions with their government.

Ari Schwartz is deputy director of the Center for Democracy and Technology where he promotes privacy protections in the digital age and expanding access to government information and services via the Internet. Cynthia Wong, a former law clerk for the Center for Democracy and Technology, is the Bernstein Fellow at NYU School of Law.

This paper was commissioned by the National Center for Victims of Crime to inform the discussion of the Panel on Technology as a Community Engagement Tool for Crime Prevention. The commissioned papers provide detailed analyses of issues related to information privacy, the handling of criminal history record information, the impact of technology on police–community relations, and e-Government. For more information, visit www.ncvc.org/ict.

Is the Information Highway a Clear Path to Better Police-Community Relations?

SOME OBSERVATIONS FROM THE BEAT AND THE STREET

by Bill Geller

Can the Internet and other electronic communications and information technology be useful to police and low-income community members whose more frequent and focused conversations, cooperation, coordination, and collaboration might make neighborhoods safer? For instance, how could such technology be used to: educate the public about reducing crime, disorder and fear; alert neighborhoods about current crime patterns so vulnerable people can take precautions; solicit neighborhood priorities for police attention; seek tips to help police investigate unsolved crimes; gain intelligence about where trouble, which could erupt into violent crime if left unchecked, is brewing; or get public feedback about police performance?

To inform the deliberations of the Panel on Technology as a Community Engagement Tool for Crime Prevention, information was collected by telephone and e-mail over three weeks in the summer of 2006 from 40 police of various ranks, 55 community developers and 10 academics and technical assistance providers. Because some respondents preferred to remain anonymous, quotations are not attributed in this working paper.

SOME CONSIDERATIONS FOR POLICE SEEKING TO USE TECHNOLOGY TO PROMOTE COMMUNITY ENGAGEMENT IN ADDRESSING CRIME

1. What are the preconditions for using the Internet and other communications technology to launch police–community anti-crime collaborations?

The means, the motive and the opportunity. To be willing to communicate with police via the Internet, community residents in crime-plagued, economically-challenged neighborhoods must have access to a computer, know how to use it, and have the time and desire to use it. Many respondents reported that in the low-income neighborhoods where they work around the nation, hardly any residents would meet all of these conditions. One respondent noted: “My neighborhood is in one of the poorest Congressional districts in America. Until recently, we had no banks. None. It’s still the only police district in our city with no parking meters. It’s a great idea to use the Internet, but how many people could we reach? Maybe we could

reach more people instead by cell phones. Even in my poor community, a lot of people have Blackberries.”

If the computer is an essential tool for the desired police–community information exchange, then, as one developer noted, one has to come to grips with the fact that “it’s expensive to own, maintain, and operate a computer with Internet access.... [The solicitation of community interaction] must be combined with a technology access service approach....”

An additional hurdle cited by most people was community residents’ reticence or unwillingness to invest trust in an unknown police officer on the other end of a computer communication. They first want to meet the officer—or some officer—face to face and be convinced that the officer and his or her colleagues can be trusted and helpful.

Most community residents in unprivileged neighborhoods, respondents said, would be weary and wary of dealing with the police because they have complained over time about crime problems, insufficient police patrols or response times, and abusive police treatment of neighborhood residents. Despite their complaints, respondents have not often noticed improvements in neighborhood safety or police activity.

Thus, a department wishing to use high-tech methods for productive two-way communication with the public would be wise to create a variety of low-tech on-ramps to the information highway. These on-ramps need to be varied to reflect the unique cultures of different neighborhoods, language and educational differences, differences in how adults and younger people learn and most comfortably communicate, and a host of other variations that constitute nuanced user-friendliness.

But average residents in fragile, challenged, or transitioning neighborhoods might, respondents allowed, be motivated to interact with an unknown officer—or even an officer whose reliability they doubt—if a trusted community-based intermediary vouched for the trustworthiness of the cops involved and the seriousness of commitment from top police officials. Still, for any such interaction to endure, the police need to follow through—by acknowledging the resident’s communication, attempting to be responsive to legitimate community requests, and keeping the resident posted on what happens to the problem at issue.

Motivating people to share ideas. Police wishing to promote Internet information exchange with the community should use a multimedia advertising campaign to make their intentions known, using, among other avenues, the broadcast news media, newspapers, and informal local communications networks. To motivate sustained participation by the community, high priority should be given to quick feedback and follow-through by the police where the request for police attention is appropriate.

One community developer said some people may be motivated enough to begin using the Internet to provide police with information and ideas because “it can be anonymous and home-based. It might be a user-friendly way for community residents to report on real problems. From the point of view of the resident, it can be very confidential. You don’t have to go anywhere to use the communications system.”

2. What preparatory work needs to be completed prior to assembling partners?

A developer recommended: “Prep work needs to be done so people will really use the system. The system has to be designed so it will not seem like Big Brother or PR nonsense. Also, the police department internally has to position this so it’s not the latest version of community policing that real cops will laugh at.” An officer opined: “For communities that don’t have elaborate engagement, start small and really involve people, then grow it. My department gets hung up on who’s the community. Just pick 10 people and start there. We don’t want to prevent people from starting by saying it has to be great.”

3. What values would you want to promote and protect as you consider different modes of communications technology to bolster police–community trust and mutual assistance?

Safety for the public. “If people without much money, who almost never use the computer, are going to have to go to an Internet café or someplace to use the ‘crime’ computer, how is this safe for the resident? How would such a high-tech system be any different than the current problem, where the cops or community leaders with cops call a meeting and nobody shows because the gang member’s girl friend is in back of the room taking notes about who’s there? We’d have to be sure the ‘cops computer’ is not physically identifiable in a chat room so everyone knows the person at the computer is talking to the cops.”

A workable feedback method. A related concern is how people whose only access to a computer is at the local library or some other such location are going to hear back from the police if the police want to reply by e-mail.

Police accountability to the ENTIRE public. A law enforcement official emphasized that there may be special ways in which the Internet’s *written* track record of communications can be beneficial to relatively powerless people when dealing with the criminal justice system: “In my area, lack of access to e-mail communication is another way in which residents are alienated from government. There is disparate access to government. If folks in a wealthy community call any public agency, they can use their political muscle, money, education to get access to top officials. The top prosecutor or police chief will shoot a memo to the local people saying, ‘Fix this problem.’ That never happens to me, as a law enforcement person, because my community doesn’t have access to the big folks.... I constantly tell folks you have to be a broken record, write a letter to the police chief. That’s how things get done. Folks get held accountable because now there’s a way to track responses to complaints. Otherwise, if you call up the department there’s no paper trail.... The Internet could provide for poor people the kind of access that the middle class already has to government.”

4. What challenges are presented for police–community linkage via Internet technology in locations with significant immigrant populations? What might work in those situations?

Language and income barriers, together with reticence to reveal crime victimization to public authorities, may inhibit police–community Internet communication in communities with non-English speaking immigrants. An Asian community developer said: “People in my neighborhood are not thirsting for information from police. All they want is for the police to clean up the streets and for things to get safer.”

Efforts to overcome language barriers are laudable and necessary (e.g., most major city Web sites post crime statistics only in English), but translations must be done with specific knowledge of an immigrant community. A cautionary tale comes from St. Paul, Minnesota, which has a large Hmong population. Several years ago, the police tried to reach out to the Hmong immigrants and had fliers translated into the Hmong language. But that didn’t help because, as the well-meaning cops learned, the written Hmong language was new. The older immigrants didn’t know how to read it.

On the other hand, there may be opportunities in some immigrant neighborhoods, as one developer suggested: there can be “huge face-losing issues in Asian communities, for instance with home invasion. The victims lose face when you bring outsiders into their crime problems. Many immigrant communities are reluctant to report, period. If the Internet encourages greater anonymity and willingness of people to tell their stories to the cops, it could be very helpful.” A number of police respondents concurred that a victim may not be able to save face when dealing with the police in person.

A police officer suggested that a useful way to involve immigrants is through radio broadcasters. “Maybe the Honduran radio broadcaster could say to his listeners, ‘The police department is working closely with me, and I want you to help them.’”

5. How would a community member know that submitting a crime report or tip to help solve a crime via the Internet would be secure and that he or she would be protected from retaliation after doing so?

One cop reflected the views of several other interviewees: “Constantly reinforce that we have the most modern technology. Anything you send to the department, only one or two people will have access to it. They are constantly supervised. We have a high level of integrity.” But still, it’s hard. “Even myself,” this officer said, “if I was going to contact the FBI or someone about an integrity problem, I wouldn’t use e-mail. What doesn’t help is when we have police officers locked up, when we have pockets of corruption. The community will ask, ‘How do we know all the cops aren’t in cahoots?’”

6. Can communications technology be used to heighten and sustain police–community efforts to safeguard low-income neighborhoods?

Technology is no *substitute* for low-tech, “high-touch” interaction. But technology may be a valuable *supplement*. Once a trusting relationship is achieved between one or more police of-

ficers and community members, it may well be useful (where the requisite computer literacy and access exist) to deepen and make more efficient their collaborative problem-solving efforts by making needed crime data and other information readily available via the Internet. As one developer who has worked in several cities noted: “In lower-income neighborhoods, the Internet is good for sharing info, not good for building relationships. It’s good to try to work at the two simultaneously by giving crime stats and other things out. But you still won’t change the relationships between police and neighborhoods using the Internet. Lower-income communities don’t use the Internet as much.”

Another developer concurred: “The Internet has made so many things so easy for us in so many ways. In some ways we’ve become spoiled in thinking the Internet can solve problems. I remain cynical. Community policing and making our neighborhood safe are difficult. There’s no easy solution. The police won’t find the Internet will make it easier. You still cannot replace the hard work of an officer really caring about the community and walking it everyday and really knowing it. Are the police trying to find an easy solution that will replace the hard work? If you think the Internet will make up for the fact that cops don’t treat people with basic respect and don’t invest in meaningful communication and assistance, forget it. Sure, if you have developed good personal relationships, and out of respect for everybody’s time, now you want to communicate by e-mail, fine. But you won’t form good relationships in that way.”

A veteran cop asked: “Technology in service of what? All the time new technology comes along and takes over (telephone, radio, guns, cars). We are mesmerized by it. For a period of time, the machines run the show. Then we realize we got mesmerized by the technology, and now we need to ask how we can really put the technology into the service of things that are important to us [such as] trying to...make your community safer. Not everybody wants to know anything about the police. Most people don’t. They want to live their lives without ever thinking about the police, because thinking about the cops means something went wrong. A lot of police departments create a big, muscular Web site that has lots of stuff on it that nobody cares about. We need to tailor the technology to serve the local interests.”

7. How do you measure success in using information technology to bolster police-community interaction?

A big-city police strategic planner said: “If, at a meeting, people say it would be useful to use the police department’s Web site to provide info, ask them what info they would like us to post. We could then do some process measurement: Did the department follow through and post the info? Then, did people find it useful? For instance, at the level of a beat, or district or neighborhood, people might ask the department about current trends on something. All of this assumes a degree of sincerity about wanting to solve problems to improve the quality of life and to use technology to solve problems. Some police agencies are serious about this and for others it’s just talk.”

Because many police agencies seek Internet links to communities to increase information exchanges between residents and the police, one basic measure of success could be to count levels of participation in contrast to attendance at beat meetings. There can be techni-

cal difficulties (e.g., in knowing how many “hits” on a Web site are from the same person as opposed to separate visitors), but perhaps technology experts could solve those problems. In Boston some years ago, a police district commander found it useful to reach large numbers of community members through a listserv the department developed at the local district level. Reporting on the experience, one interviewee said: “Some computer guys in District 4 started a listserv which at one point had 500 people on it, between the police and the community. Information and ideas flowed back and forth.... It kept participation levels up because all a resident needed to hear from a neighbor was ‘I sent them an e-mail and got an answer 24 hours later.’”

8. How could a police department enable community residents to file and track complaints about the police using the Internet?

Is the information highway that police seek to build between themselves and communities a one-way street? While police hope to receive crime-solving tips from the community, are they also willing to receive tips from the public about officers engaging in possible misconduct?

One community developer suggested: “There’s no reason [the Internet] couldn’t be an effective way to report complaints, so long as it’s not just general. It must be very detailed, and the complaint can’t be made public. The concept that you constantly have to go to the police in their fortress is not good. Complaints by e-mail could be a way of removing some of the moats and drawbridges.” A police official commented: “There’s a great deal of mystery to the police complaint process.... A department can take a lot of the mystery out of it by saying ‘Come on and complain.’ But we have to provide meaningful fields in the online complaint form so the ridiculous complaints are filtered out.”

A police official suggested possible benefits of allowing the public to file complaints online: It’s a nice convenience to be able to collect one’s thoughts and then write in a complaint, whether it helps to decompress from a stressful encounter with police, gives a greater sense of anonymity, or is simply a convenient mechanism for the complainant. We receive some through our Web site, but not many. The majority of dissatisfied people call in their complaints directly to IA [Internal Affairs], talk to a supervisor or complain in person. To some degree, I think it helps elevate trust if people know the avenue [Internet] is available, and it also provides clear information about how the process works.”

If departments open their Web sites for the public to file complaints, it would be sensible to also allow the public to file commendations of police officers who gave good service. And it may be valuable to allow people to make complaints and commendations of the whole police department. “In reality,” a former police Internal Affairs commander suggested, “many complaints against individual officers are really complaints against Department procedures and policies. Someone in IAD could post each week on the Internet the number and type of complaints filed and the status of those investigations (without identifying the specific people involved). Once that is done, the whole thing will lose its mystery and scariness. We need to achieve fairness and decent motives on all sides.”

In fact, many police departments do provide places on their Web sites for the public to offer complaints and compliments about police actions. It may be possible for police departments also to e-mail status reports to complainants who used the Internet to file complaints. This is simply another means, besides telephone, for an internal affairs investigator to update the complainant.

9. Do various cities provide citizens with crime data via the Internet, and if so, how current is the information? What do police and community development practitioners think is the value of providing crime data via the Internet?

Some doubt the value of sharing crime data with the community. “Our police department lately wants to give us stats,” said one community developer. “Who gives a damn that the stats are down if I still have a drug dealer when I walk out the door? I don’t care that you’ve made 20 arrests.”

But many respondents favor the provision of current crime statistics, with some caveats. As one community organizer put it: “It would be a good idea, so long as there is a strong partnership already to address the results of the crime analysis and a commitment to work together on the issues highlighted by the data.” Another community organizer cautioned: “It can be good to have that info out there. But it also can be harmful, especially crime stats showing a jump in crime if there is no way for people to respond to that info in real time. A monthly district-wide meeting isn’t going to cut it.” She added: “The crime stats have to be current. It won’t help the community to find out mid-July there was a rash of break-ins in the first two weeks in June. That will just tick people off rather than help them.”

Many police said they think posting crime statistics on the Internet is a good idea. But some concurred with one cop’s admonition: “It’s important also to explain the stats. Our department doesn’t put arrest stats on the Web site. [But] if the web shows our violent crimes are up, the community should also know that we’re working on it—our robbery arrests and gun arrests are up.”

A community organizer based in a community development corporation (CDC) noted: “Some CDCs won’t like to see the neighborhood be up on the Internet with crime stats—they are trying to change the rep of the neighborhood, and this just confirms it’s dangerous. If the police, CDCs, and other neighborhood groups can sit down together and talk about what info is best for both, the info can be valuable.”

A veteran police manager had doubts about the usefulness of the kind of monthly crime statistics offered by many police departments to the public—generally aggregate listings of the number of FBI-defined Part 1 felonies that occurred within a police precinct or district. He contrasts FBI Uniform Crime Report (UCR) data with data that are available to police—but rarely are made available in a timely fashion to the public—generated by NIBRS, the National Incident-Based Reporting System: “How valuable is it to get more of the info devised in 1929 more quickly? I think it’s outmoded. In NIBRS, more info is captured about the actual nature of the offenses, instead of burying it all under a hierarchy of crime classifications.” A developer shared the view that traditional UCR crime statistics aren’t very helpful: “Does it matter to me to understand whether the victims were two elderly people or

two drug dealers? Yes. If it was dealers, now I know there's a drug war. But I especially care if the people killed were elderly because you wouldn't expect them to be killed. If the police just tell me two people died, I say, "Two what?"

Even those who doubt that UCR crime data are informative to communities admitted that there can be some ancillary value to making such data publicly available. Said one police officer, "It shows some willingness on the part of the police department to reach out. The info is not so valuable, but the fact that the police are making the effort would impress me as a community member."

Another police officer wondered if police Web sites or other Internet tools could be used to clarify police enforcement priorities. One example, he said, might be traffic enforcement priorities: "In terms of information technology and what kinds of info should be provided by police to the community, let's assume that traffic stops have a positive effect on traffic calming. Could we use the Internet to explain why a police department does ticketing—come clean on our actual policy? The public doesn't know what the real speed limit is until they get pulled over."

Perhaps the Internet could be used also to help the public recommend ways that police could be more effective in fighting crime, disorder, and fear. "Maybe," said a police respondent, "if we present the public with information—not just data—about what we're trying to accomplish by addressing certain kinds of crime, the public could imagine how we could do better."

Early in the 21st century, private-sector organizations in the United States use a vast network of information superhighways to communicate with customers, collaborators, and other stakeholders. By comparison, the use of information technology in most police agencies and other criminal justice organizations is at a more rudimentary stage of development. Over time, as police attempt to upgrade from unpaved roads to information highways in linking to their service populations, they may find their paths clearer if they address the kind of considerations raised by our street-wise respondents.

Bill Gellar is director of Gellar & Associates Consulting and provides technical assistance and training on effective community policing.

This paper was commissioned by the National Center for Victims of Crime to inform the discussion of the Panel on Technology as a Community Engagement Tool for Crime Prevention. The commissioned papers provide detailed analyses of issues related to information privacy, the handling of criminal history record information, the impact of technology on police-community relations, and e-Government. For more information, visit www.ncvc.org/ict.

Privacy Issues for Online Community Policing

by Ari Schwartz and Cynthia Wong

INTRODUCTION

Online tools to expand community engagement in crime prevention offer exciting possibilities but also raise significant policy issues. In some cases, tools intended to empower citizens to participate more actively in crime prevention can trigger privacy concerns both for users and for individuals who have had contact with the criminal justice system.¹ This paper addresses the privacy concerns of users of online systems.

Privacy is a critical enabler of trust, both online and offline. Establishing strong trust relationships between stakeholders and police officers is just as important to community involvement online as it is in the offline world. Unless individuals believe their privacy and security will be protected, they will be wary of allowing personal information to be collected and used and so may not participate. Similarly, community members will be less likely to use online community policing services unless they are assured that the information the government collects will be used responsibly and will be protected from abuse.

To promote trust in online community policing and encourage broad use of such systems, officials should address privacy issues in all phases of planning, design, implementation, and evaluation. Going into each project, law enforcement officials should work with the community to assess possible impacts on privacy in accordance with fair information practices and should strive to mitigate adverse effects.² Because these systems will be used as one tool in a larger structure of community policing, they should be employed in a way that strikes an appropriate balance between users' interest in privacy and the community's interest in effective community policing.

¹ When information about penitentiary releases, parolee releases, arrests, and locations of crimes is published online, privacy issues arise with respect to a variety of individuals. This paper will focus on privacy issues for users of the CAPS system (and other similar online policing efforts) and will not address issues surrounding criminal history information or ex-offender releases.

² See Privacy Basics: Fair Information Practices, CDT's Guide to Online Privacy, Center for Democracy & Technology, <http://www.cdt.org/privacy/guide/basics/fips.html> (accessed July 25, 2006).

PRIVACY ISSUES THAT TECHNOLOGY RAISES

Identity and Authentication³

When developing systems that enable community members to share information with local beat officers, a paradox arises: an individual will be more willing to report problems and provide feedback about police conduct or city services, if he or she is allowed to do so anonymously. However, enabling anonymous reporting could invite abuse of the system and lead to problems where such false reporting results in investigations of crimes, deployment of city services, or referrals to social service agencies.

In the offline context, community policing programs have addressed this problem by creating mechanisms where individuals can report information with accountability and also with a sense of anonymity. For example, community members can attend beat meetings where they are encouraged, but not required, to sign in, and no one is asked to show identification. However, attendees participate in a public setting where a beat officer can remember their face. This is by no means a perfect solution. A drug dealer could attend the meeting for the sole purpose of intimidating those who may report illegal activities to beat officers. Also, an individual from outside the community could come in and blame law-abiding community members of illegal behavior with little accountability. However, this system does provide some sense of balance. An online mechanism for community policing should provide a similar balance between the need for accountability through authentication and participants' desires to protect their identities.

In general, users should be able to access public information and online services without having to register. If users do register (or are required to register) to receive beat-specific updates or to access services, officials should work with the community to establish guidelines prior to the launch of a system to protect personally identifiable information associated with the e-mail addresses and pseudonyms the system collects. Moreover, such systems should only collect the personal data necessary to provide users with the services or functionality they want to use, and the personal data should only be retained or used for those purposes. For example, submitting comments to a beat meeting should not require the submission of much personally identifiable information, if any. On the other hand, in situations where users are reporting information that could implicate the privacy or freedom of others—for example, reporting domestic abuse complaints that could trigger child protective services or reporting possible offenders by name—it may be necessary to collect some general data while allowing users to hide their identities with pseudonyms. Community policing programs must create clear policies on how this information will be treated in the course of a possible investigation to properly balance the user's desire to participate anonymously or pseudonymously with the alleged offender's due process rights.

³ "Authentication" is the process of establishing confidence in the truth of some claim. This often includes use of identity information, but it may not need to. The canonical example of anonymous authentication is the signs at amusement parks that say "you must be this tall to ride this rollercoaster." The ticket agent never learns the identity of the individual but can tell if they meet the height requirement. The National Academies have produced a detailed study, *Who Goes There?: Authentication Through the Lens of Privacy*, (Washington, DC: National Research Council, National Academy Press, 2003).

In some circumstances, it may be necessary for law enforcement to identify pseudonymous participants. For example, as a case moves through the criminal justice system or across city agencies, the police may need to identify the source of evidence gathered online (for example, through the Web “tip” system). Guidelines that delineate the circumstances in which (and to what extent) law enforcement may use its power to identify such participants should be determined prior to the creation of these systems and communicated to users when they register or submit personal data.

Security of Information in Transit

Polling information suggests that many Internet users are concerned about the security of personal or confidential information as it is transmitted across cyberspace, and they are cutting back on their use of the Web because of these concerns.⁴ The rise of “keyloggers” and other “spyware” programs that capture information for hackers and illicit uses has increased this concern and made real many of the public’s worst fears about transmitting sensitive information online. Police departments should realize the severity of this threat by encrypting data flows where sensitive data is transmitted and encouraging the use of security patches and updated anti-virus and anti-spyware technologies both within the department and among the community.

Location Information and Surveillance

Many computer users have an expectation that they can keep their physical location (where they are when using their computer or a mobile device) a secret. In reality, information can sometimes be used to pinpoint the general location of an individual through their Internet service provider. With more transactions occurring through mobile devices, such as smart phones that use location-based information for calling and emergency purposes, location-based services, such as mapping, and information are becoming widespread.

In the future, police departments may offer location-based services, which may require users to transmit location information to the police. Such features would raise privacy issues related to location information and police surveillance. Moreover, a wireless service provider’s logs may store cell site information retrospectively, allowing anyone with access to trace callers’ past movements. New phones that incorporate GPS technology enable even more precise tracking capabilities.⁵ Such systems would be consent-based, but their logs might be sought for other purposes.

Finally, releasing location information on individual crimes raises a range of issues that should also be addressed before this information is made widely available online. Online publication of the specific locations of crimes may give rise to a violation of privacy for victims of crime, in addition to increasing chances of re-victimization or embarrassment if crime

⁴ See “Leap of Faith: Using the Internet Despite the Dangers,” by Princeton Survey Research Associates International, for Consumer Reports WebWatch, October 26, 2005. Available at <http://www.consumerwebwatch.org/dynamic/web-credibility-reports-princeton.cfm>.

⁵ See Center for Democracy & Technology, “Digital Search & Seizure: Updating Privacy Protections to Keep Pace with Technology,” (February 2006), 19–30, available at <http://www.cdt.org/publications/digital-search-and-seizure.pdf>.

location data is too specific. For example, at a community meeting that we attended during the CLEARpath process, we were told of a recent case where a civilian paid by the Chicago Police Department had sent the home address of a sexual assault victim in an e-mail to the entire neighborhood list. This incident raised major privacy concerns and provoked community outrage at the CPD. The Center for Democracy & Technology suggests that published crime mapping should remain limited to the beat or block level and should not include specific addresses. Moreover, publication of arrest information may invoke both due process and privacy concerns for individuals who have been accused of crimes because of the stigmatizing effects such publication may have.

Data Retention and Use Limitations

As community policing systems store data for analysis, such storage raises new concerns about how long personally identifiable information will be retained and the extent to which law enforcers can use such information for purposes other than those for which it was originally collected. One of the main features of community policing programs is their beat-specific, problem-solving approach. A long-term understanding of chronic and persistent problems specific to a neighborhood is vital to the formulation and success of any community-wide response. The online systems envisioned for community policing would enable collection and sharing of information among different community and city stakeholders. This increased information flow would allow community leaders to work together on solutions involving multiple city agencies, community-based organizations, and residents. However, because personal data can be retained and shared so easily, limitations on its use and redistribution need to be clearly delineated in privacy policies and strictly enforced. Use limitations are especially important as data is shared across city agencies and community organizations with differing standards for protection and retention of data. While some information may need to be retained for internal police or social services purposes, personal information on specific users should not be kept (or made publicly available) any longer than is necessary for the function in question. Ongoing and periodic assessments of the relevance of retained data are important because it is difficult to predict how data will be shared and managed across multiple departments and users, especially because data collected for one purpose is often used for other purposes.

Indeed, information collected for one purpose is often used for another despite the best wishes of the creator of the system. While a community policing project should include in its privacy policy limitations on how third parties may use personal data, this policy alone is not enough to ensure that such restrictions will always be followed or respected, even with necessary enforcement mechanisms. This concern includes both internal decisions to release data for unforeseen purposes and information accessed illegally, such as the theft or hack of a system that includes personal information.

The best privacy policy is always to avoid collecting information that is not specifically necessary for a stated purpose.

Also, if departments release certain user data to third parties, privacy officials should give advance notice to affected users and seek their consent. If user information is breached, privacy officials should give notice of the breach to affected parties as soon as possible. Users

should have the ability to control how their personal data is used to the fullest extent possible. If data is released to third parties, users should be able to receive a copy of the data released for free or at low cost.

GENERAL RECOMMENDATIONS

1. Build a Privacy Compliance Program

Addressing privacy concerns as community policing moves online requires privacy compliance programs that are incorporated into all phases of planning, design, implementation, and evaluation. An effective privacy protection regime will also include mechanisms for training, oversight, and enforcement.

Police departments should establish a privacy office with a Chief Privacy Officer (CPO). With adequate staffing, the CPO would be charged with developing privacy policies for all aspects of the online system; conducting privacy impact assessments; training officers, community policing staff, and volunteers; overseeing the implementation of privacy initiatives; and enforcing policies.

The privacy office in a police department should also act as an independent gatekeeper by controlling access to sensitive user information according to relevant surveillance standards and fair information practices. For example, if a police officer wishes to identify an anonymous or pseudonymous user as a part of an investigation, internal procedures could require investigators to obtain the approval of the CPO before seeking the information. Such a consultation may lead to the conclusion that maintaining public trust in the system outweighs any value in identifying the user. This procedure should not be made overly complicated.

*It may also be desirable to create a Privacy Commission as an independent city or state entity charged with overseeing privacy policies, investigating legal compliance, and consulting with other relevant agencies.*⁶ At a minimum, there should be some type of privacy coordination body outside of the police department, as community policing is a citywide initiative that spans across many different agencies and departments.

CPOs or chief privacy contacts must work with the privacy commissions or the appropriate coordinating bodies to ensure that all agencies and departments involved in community policing data collection understand and comply with privacy policies. Privacy departments should provide training as necessary for officers and other agency officials. Privacy training should not only present privacy policies and procedures, but also the rationale behind these policies. Officers and other community policing staff will be more likely to comply with privacy protections if they understand why personal information is sensitive and the potential consequences that may result when privacy interests are compromised.

⁶ For example, in Canada, all of the provinces have independent privacy commissions. Ontario's data commissioner, Ann Cavoukian, frequently works with municipalities and the provincial police on their implementation of new technologies. In the United States, the California Office of Privacy Protection also regularly works with law enforcement on privacy issues.

2. Assess Impact on Privacy

All new technologies and projects should undergo privacy impact assessments (PIAs) to assess the effects they may have on individual privacy and to determine how any adverse effects may be mitigated. In general, a PIA will include a description of the proposed project, the types of personal data that will be collected or used, and how data will be disseminated or retained. To the extent that the proposed action or program is found to pose a risk to privacy, the PIA reviews the technical, procedural, or other safeguards that can be adopted to protect privacy and recommends how to implement the system in a manner consistent with fair information practices. PIAs are typically written by program managers and approved by CPOs.⁷

3. Post Clear Privacy Policies for All Projects

The CPO should post clear privacy policies in plain English (at a fifth-grade reading level) for both internal and external users. For internal users, policies should be provided as a part of privacy training. For external users, privacy notices and policies should be posted on community policing Web sites and should be accessible from pages where personal data is collected. Privacy notices should explain what personal information may be collected; how it will be used, stored, and disclosed; and how long the information will be retained. The goal of privacy notices should be to give potential users sufficient information to decide if they want to proceed with providing their personal information online, use another method of participating in community policing programs, or opt out. The notices should also include information on accountability procedures for individuals who believe that personal information may have been misused.

4. Develop Mechanisms for Internal Quality Control

The CPO should develop mechanisms and internal checks to maintain the quality of community policing information. Police departments should seek to ensure that data collected about users and information provided to the community through government Web sites is complete, accurate, and up to date. Online community policing projects should be designed so that data can be easily and efficiently verified and corrected under appropriate authority. Such systems may entail methods for cross-referencing, data analysis to identify anomalies, authorized human correction, and evaluation of record retention and use limitations. Internal evaluation and correction of data must be traceable to authorized users as a part of developing an audit trail that would enable ongoing impact assessments.

5. Develop Measures to Minimize Collection, Data Retention, and Unauthorized Secondary Use

CPOs should create mechanisms for internal checks on how information is used. More specifically, CPOs should develop measures to minimize collection, data retention, and unauthorized secondary use wherever possible. Ongoing assessments about what data should be collected and how long data should be retained are necessary as new information gatherers (e.g., third-party data aggregators) and users emerge. Systems must be designed to stop or

⁷ The E-Government Act of 2002 requires PIAs for all U.S. federal government agencies that perform new data collections affecting ten people or more.

minimize unauthorized uses of personal data because it cannot be assumed that information collected for one purpose will not be used or shared for an unrelated purpose.

Toward that goal, CPOs should develop:

- Authorization procedures for data access, even for users internal to the criminal justice system;
- Protocols that track who has accessed information and for what purpose;
- Audit trails to enable ongoing impact assessments;
- Policies and procedures that govern disclosure and redaction as information moves from one audience to another; and
- Mechanisms for authorized updates and corrections.

6. Develop Measures to Minimize Misuse of Data by External Third Parties

The CPO should develop measures to minimize unauthorized access to and misuse of data by external third parties. As a general rule, disclosures to third parties should be avoided. Where data could be released to third parties—either private or commercial entities or external city agencies—agencies should notify affected users and obtain consent where appropriate. Privacy teams should allow users to access a copy of any personal data that was released (for free or at a low cost) and provide an opportunity to correct errors. The CPO should also develop guidelines and restrictions for how such third parties may use or redistribute released data.

7. Engage and Respect Community Views on Privacy

The success of a community policing program lies with its ability to engage the community in collective problem solving. The online component of community policing should respect community views at least as much as its real-world counterpart. Going into each project, the CPO should fully vet privacy implications with the community. This ongoing dialogue educates the community about privacy issues and increases transparency around the collection and release of different types of information. Engaging the community on privacy issues helps build trust between the police and local communities, which in turn increases the chances of wider participation in, and therefore the effectiveness of, online community policing.

Ari Schwartz is deputy director of the Center for Democracy and Technology where he promotes privacy protections in the digital age and expanding access to government information and services via the Internet. Cynthia Wong, a former law clerk for the Center for Democracy and Technology, is the Bernstein Fellow at NYU School of Law.

This paper was commissioned by the National Center for Victims of Crime to inform the discussion of the Panel on Technology as a Community Engagement Tool for Crime Prevention. The commissioned papers provide detailed analyses of issues related to information privacy, the handling of criminal history record information, the impact of technology on police–community relations, and e-Government. For more information, visit www.ncvc.org/ict.



Privacy Considerations

A FOCUS ON CRIMINAL HISTORY RECORDS

by Bob Belair

WHAT IS PRIVACY?

What is privacy? That question has intrigued and, frankly, bedeviled generations of privacy scholars and lawyers.¹ Privacy is best thought of in three categories. The first category is behavioral privacy—the freedom to engage in conduct without unreasonable restriction. Over the course of time, that concept has emerged as a sort of proxy for freedom, undergirding religious freedom, reproductive freedom, and other very personal behavior.²

The second bucket, “surveillance privacy,” is a related, but still distinct, category. Americans have always worried about “Big Brother”—about being watched, or listened to, or investigated. This branch of privacy has its roots in the Fourth Amendment’s protections against unreasonable searches and seizures.³ Numerous and important Supreme Court opinions address the “right to be let alone,” sometimes by interpreting surveillance as a “search” within the meaning of the Fourth Amendment and, more recently, by measuring whether the individual had a “reasonable expectation of privacy” against government surveillance.⁴ There are today, for example, relatively expansive constitutional, statutory, and common law protections against government wiretapping and eavesdropping.⁵ Indeed, a federal court recently declared the president’s secret eavesdropping program unconstitutional on the grounds that it violated the Fourth Amendment’s privacy protections.⁶

In the computer era, a third branch of privacy emerged—“information privacy.” Information privacy refers to an individual’s ability to control, or at least to participate in, deci-

¹ See, generally, Krotoszynski, Ronald. “Autonomy, Community and Tradition: A Contrast of British and American Privacy Law, 1990 Duke L. J. 1398, December 1991; see, also, Brandeis, Louis and Samuel Warren, “The Right to Privacy,” 4 Harvard Law Review 193 (1890).

² See, *Roe v. Wade*, 410 U.S. 113 (1973)

³ U.S. Const. Amend. IV; *Olmstead v. U.S.*, 277 U.S. 438 (1928) (Justice Brandeis’s dissenting opinion was a keystone of the Supreme Court’s later recognition of broad privacy rights).

⁴ See, *Katz v. U.S.*, 389 U.S. 347 (1967).

⁵ See, *U.S. v. Koyomejian*, 946 F.2d 1450 (1991) (containing a thorough discussion of the Foreign Intelligence Surveillance Act (FISA) and Congress’s intent to expand the privacy protections recognized by the *Katz* Supreme Court decision).

⁶ Associated Press. “U.S. Judge Nixes Warrantless Wiretaps” available online at <http://www.cbsnews.com/stories/2006/08/17/politics/main1904506.shtml>.

sions about the collection, maintenance, use, and dissemination of his or her own personally identifiable information.⁷ In 1977, the concept received landmark recognition when the Supreme Court declared that, although the government was free to collect information about individuals and use the data in a reasonable manner, the government could not disseminate or disclose private information about individuals without legal cause.⁸ Around the same time, Congress recognized privacy rights in the commercial use of information by enacting the first version of the Fair Credit Reporting Act.⁹ Other citizen and consumer information privacy statutes, including the Privacy Act of 1974¹⁰ and the Family Educational Right and Privacy Act,¹¹ soon followed. More recently, the Congress has enacted important protections for health records and financial records.¹²

FAIR INFORMATION PRACTICE PRINCIPLES

In the early 1970s, two important studies developed the concept of “Fair Information Practice Principles” (“FIP Principles”).¹³ As information privacy has evolved, it has come to mean more than simply confidentiality. The key elements of the FIP Principles are:

- Notice or transparency;
- Limits on collection of information;
- Assurance of data quality;
- Use and compatibility controls;
- Consumer choice and confidentiality;
- Access and correction;
- Accountability;
- Dispute resolution; and,
- Data security.¹⁴

⁷ See, Westin, Dr. Alan. “Privacy and Freedom,” New York: Atheneum (1967).

⁸ See, *Whalen v. Roe*, 429 U.S. 589 (1977).

⁹ 15 U.S.C. 1681 et seq.

¹⁰ 5 U.S.C. 552a et seq.

¹¹ 20 U.S.C. 1232g; 34 CFR Part 99.

¹² The Health Insurance Portability and Accountability Act (HIPAA), 42 U.S.C. 1301 et seq., contains provisions governing the use and dissemination of personal health information. The Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. 6801 et seq., and its regulatory framework require financial institutions (broadly defined) to strictly safeguard consumer financial and personal information. GLBA regulations also require financial institutions to notify consumers whose information has been exposed to potential identity thieves due to a breach of security of the financial institution’s personal information safeguards. For more information, visit the Federal Trade Commission’s website at <http://www.ftc.gov/privacy/privacyinitiatives/glbact.html>.

¹³ See, Westin, Dr. Alan. “Databanks in a Free Society,” New York: Times Books (1972); See also “Records, Computers, and the Rights of Citizens: Report of the Secretary’s Advisory Committee on Automated Personal Data Systems,” available online at <http://www.epic.org/privacy/hew1973report>.

¹⁴ Federal Trade Commission. “*Fair Information Practice Principles*,” available online at <http://www3.ftc.gov/reports/privacy3/fairinfo.htm>.

In the past two years, data security has erupted as the hottest privacy topic. Between March 2005 and September 2006, nearly 300 information security breaches have been reported by universities, businesses, and government agencies.¹⁵ As a result, the personal information of as many as 90 million Americans has been exposed, leaving those consumers more susceptible to identity theft.

THE PRIVACY ENVIRONMENT

Today, the public is more worried about privacy than perhaps ever before.¹⁶ The public is especially worried that their personal information will be captured and misused for identity theft—America’s fastest-growing crime.¹⁷ And, to make matters worse, the public is barraged with stories about radio frequency identification technologies, biometrics, GPS tracking technologies and many other new surveillance and information and identification technologies which have further fanned the public’s privacy worries.¹⁸

Privacy concerns are especially high when it comes to the Internet—the public commonly complains about a “sense of being watched” on the web.¹⁹ With about 90 million users online every day, it’s a troubling sign for e-commerce that 92 percent are “worried” about privacy on the Internet, with 72 percent describing themselves as “very worried.” In fact, some believe that more than half of Internet users refrained from making an online purchase because of concerns about privacy or identity theft,²⁰ and an equal number have refused to make an online purchase because of concerns about privacy or identity theft.²¹

PRIVACY AND CRIMINAL HISTORY RECORDS

The public is also concerned (though slightly less so) about the availability of criminal history information on the web. For example, some surveys show that as much as 90 percent of the public is opposed to posting criminal conviction data—other than sex offender data—on the Internet.²² But, take the Internet out of the equation and the public seems to reverse itself—approximately 90 percent support public access to conviction information, at least in particular circumstances—depending upon the purpose for which conviction data will be

¹⁵ For a comprehensive, up-to-date list of information security breaches, visit <http://www.privacyrights.org/ar/ChronDataBreaches.htm>.

¹⁶ U.S. Department of Justice, Bureau of Justice Statistics, “Report of the National Task Force on Privacy, Technology and Criminal Justice Information - Public Attitudes Toward Uses of Criminal Justice Information.” August 2001, p. 33 (available online at <http://www.obblaw.com/privacytfreport.pdf>).

¹⁷ According to the Federal Trade Commission. See, www.ftc.gov and www.consumer.gov/idtheft/.

¹⁸ See, <http://www.epic.org/privacy>.

¹⁹ David Shenk, “A Growing Web of Watchers Builds a Surveillance Society.” *New York Times*, Jan. 25, 2006. Available online at <http://www.nytimes.com/2006/01/25/technology/techspecial2/25essay.html?ex=1295845200&en=153c2477828e98a7&ei=5088&partner=rssnyt&emc=rss>.

²⁰ U.S. Department of Justice, Bureau of Justice Statistics. “*Privacy, Technology, and Criminal Justice Information: Public Attitudes Toward Uses of Criminal History Information - Summary of Survey Findings*,” July 2001, p. 4. Available online at <http://www.obblaw.com/privacytfsurvey.pdf>.

²¹ Cyber Security Industry Alliance poll, April 20-27, 2006. Available online at https://www.csalliance.org/publications/surveys_and_polls/dci_survey_May2006.

²² *Supra*, note 18, at 5.

used and what type of offender is at issue (minors, violent offenders, etc.).²³ This difference has led some skeptics to conclude that what the public actually favors is *practical obscurity*. In other words, the public favors data availability in theory but favors confidentiality in practice.

In any case, however, the public is almost unanimously in favor of applying fair information practice principles to criminal history data.²⁴ For example, about 90 percent believe that an individual should be able to access his rap sheet, dispute inaccuracies and have it corrected, when appropriate.²⁵ Eighty-five percent also agree that an individual ought to be notified when his criminal history records are accessed by a third party.²⁶

As mentioned above, however, the public does recognize important distinctions among different types of criminal history data. The public, for instance, makes a sharp distinction between conviction data and arrest data.²⁷ As a further example, and as noted, while the public strongly disfavors Internet availability of most criminal history data, the public is almost unanimous in its support of Internet access to sex offender information. Polling indicates that the public also disfavors public availability of witness and victim data, intelligence and investigative data, and juvenile data.²⁸

The public's thinking about offenders' rehabilitation and their reentry into society also carries significant privacy implications. Since 1990, the number of people in our nation's jails and prisons has nearly doubled—about 6.9 million adults are currently incarcerated or on probation or parole (the highest rate of any country in the world).²⁹ Each year, about 654,000 people are released from jail, prison or other incarceration.³⁰ That works out to be nearly 1,800 people per day. Sadly, however, recidivism rates among newly released offenders are high—way too high. Of the hundreds of thousands of people released from prison each year, most of them commit a felony or serious misdemeanor within three years of release.³¹

In addition, the cycle of incarceration, recidivism, and “re-incarceration” hits hardest at minorities. About 18.6 percent of black males will enter prison during their lifetime. The number is 10 percent for Hispanic males.³²

The case for confidential treatment of criminal history data is strongest when addressed to events that occurred ten or more years earlier. Research indicates that if an offender has a clean record or a record with no criminal activity for ten years past incarceration, the offend-

²³ *Id.*

²⁴ *Supra*, note 14.

²⁵ *Supra*, note 18, at 5-6.

²⁶ *Id.* at 6.

²⁷ *Id.* (66% of the public distinguish between access to conviction records and access to arrest records of persons not convicted.)

²⁸ *Id.*

²⁹ U.S. Department of Justice, Bureau of Justice Statistics. *Correctional Surveys*, available online at <http://www.ojp.usdoj.gov/bjs/glance/corr2.htm>.

³⁰ U.S. Department of Justice, Bureau of Justice Statistics. *Criminal Offenders Statistics* available online at <http://www.ojp.usdoj.gov/bjs/crimoff.htm#recidivism>.

³¹ U.S. Department of Justice, Bureau of Justice Statistics. *Criminal Offenders Statistics* available online at <http://www.ojp.usdoj.gov/bjs/crimoff.htm#recidivism>.

³² U.S. Department of Justice, Bureau of Justice Statistics. *Criminal Offenders Statistics* available online at <http://www.ojp.usdoj.gov/bjs/crimoff.htm#prevalence>.

er is unlikely to recidivate.³³ Based, at least in part, on this research, most states have adopted standards for sealing and/or purging some or all aged conviction data.³⁴

THE PUBLIC INFORMATION ENVIRONMENT

Public information nourishes important societal values and interests. For instance, public access to personal data promotes the “meritocracy” by helping decision makers, including employers, licensing boards, credit grantors and many others to make better decisions – decisions that are objective and fair and that reward hard work and achievement. At the same time, public access to personal data also aids in holding persons accountable for inappropriate, harmful or criminal actions. Public access to personal data also enhances government oversight, provides better information for risk management, and promotes public safety and homeland security.³⁵

Public opinion about openness to criminal history record information pivots on the content of the criminal history record information and the proposed use of the criminal history record information, rather than on the *source* of the criminal history record information.³⁶ However, under pressure from a growing army of non-criminal justice users, federal and state governments continue to enact new laws mandating or authorizing criminal history background checks for new purposes such as port security, airport security and to screen handlers of hazardous materials.³⁷ By and large, survey research indicates that the public supports these efforts. This is reflected in the introduction of about 20,000 criminal history background screening bills in Congress and in the states since 9-11. Three thousand have been enacted during that span.

THE TRANSITIONAL ENVIRONMENT

What are the key trends today in criminal history information law and policy?

- Artificial legal distinctions based upon the source of criminal history record information are eroding. Instead, in the future, privacy distinctions are likely to be based upon content and use.
- FIP standards are a better fit for consensual data bases, rather than for non-consensual databases. (It is counter-productive, for example, to give offenders “choices” when it comes to their criminal history records. In other words, giving offenders the opportunity to opt-out of a criminal history database would, inevitably, “gut” the database.) Over the next several years, it is likely that new FIP standards for non-consensual databases, including criminal history record information, will emerge.

³³ Richard Freeman, “Employment Dimensions of Reentry.” Urban Institute Reentry Roundtable, May 19-20, 2003. P. 8.

³⁴ See, www.removeit.org/eligibility.

³⁵ *Supra*, note 18.

³⁶ *Id.*

³⁷ Over 100 bills introduced in the 109th Congress related to the use of criminal history information. Search at <http://thomas.loc.gov>.

- The role of the Internet is still growing and changing, but we can expect that, thanks to the Internet, it will become easier and cheaper to check criminal history record information. It's also likely that, in many circumstances, individuals will be able to monitor who has checked their criminal history record information.
- The role of criminal history information for various non-criminal justice applications continues to grow, but also continues to generate controversy. Some uses appear to have broad support (background checking for individuals providing services to children), while other uses cause concern. For example, there has been widespread concern that programs like REAL ID and new employment background checks for aliens will generate inappropriate demands for access to and use of criminal history record information.³⁸
- International sharing of criminal history information is expected to increase but also expected to be controversial.³⁹
- Investigative and intelligence data is likely to remain unavailable to the public for two reasons: (1) it is often unreliable; and (2) exposure of investigative or intelligence data may compromise investigations.
- Victim, witness and juvenile adjudication information is likely to be at least partly unavailable to the public. Records of older juveniles who commit serious offenses are likely to be publicly available.
- Over the next ten years, adult criminal history record information, including arrest data, is likely to be fully and immediately available to the public via the Internet (or through comparable, automated means).

PRIVACY PROTECTIONS IN AN INFORMATION ENVIRONMENT

Many information scholars believe that the challenge for the first quarter of the 21st century is to balance public availability of criminal history record information with sufficient confidentiality protections to promote offender rehabilitation and reintegration.⁴⁰ However, in an era of automated court records; automated news morgues; and Google, Yahoo and other robust Internet search engines, will it ever be possible to cloak an individual's criminal history record with confidentiality protections? The answer, almost surely, is "no."

Instead, if we assume that America is moving—and rapidly moving, at that—toward an environment of total criminal history record information availability, are there privacy-sensitive and ameliorating steps that can be taken to promote fairness and reintegration? The answer, almost surely, is "yes."

³⁸ For a concise summary of these concerns, visit http://www.epic.org/privacy/id_cards/.

³⁹ U.S. International Crime Control Strategy available online at <http://clinton4.nara.gov/WH/EOP/NSC/html/documents/iccsfrm.html>.

⁴⁰ See, e.g., Solove, Daniel. "The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure," 53 Duke L. J. 967, December 2003; Geiger, Ben. "The Case for Treating Ex-Offenders as a Suspect Class," 94 Calif. L. Rev. 1191, July 2006.

- *Fair information practices.* Criminal history record subjects should enjoy comprehensive and robust FIP protections including, in particular, protections on the accuracy of their criminal history record information; full access rights; full correction rights; a right, in most instances, at least, to see who has acquired their criminal history record; and the opportunity to append a narrative to the criminal history record, emphasizing mitigating factors, such as an extended clean record period or various extenuating circumstances regarding the criminal history event.
- *The nation should promote criminal history record literacy.* Today, most laymen have difficulty reading and understanding a “rap sheet.” Frequently, for instance, the charges listed on an individual’s record do not match up with the offenses for which an individual has been convicted. This causes a good deal of confusion on the part of those who read and use criminal history records. As the criminal history record becomes increasingly available to the public, the chances of misinterpretation and misunderstanding increase. It is important that we find ways to enhance criminal history record literacy so that readers and users of rap sheets understand the information and are able to place the information in context.
- *Restrictions on the use of criminal history record information.* Already, we are seeing in several states restrictions on employers’ ability, for example, to use criminal history record information to make employment decisions. Those kinds of restrictions customarily pivot upon the offender’s age at arrest or conviction; the severity of the offense; the frequency of criminal behavior; the length of time that has elapsed since the last episode of criminal behavior; evidence of rehabilitation; and any other relevant and extenuating circumstances. The existence of a criminal history record need not be an automatic bar to employment, insurance, credit, licensing or other valuable rights and statuses.
- *The nation should consider the adoption of “certificates of rehabilitation” that would be awarded to offenders who meet the metrics for these certificates.* A certificate of rehabilitation would assist offenders in obtaining employment and other valued statuses. These certificates would also give comfort to employers and others who are providing privileges to offenders.
- *Government-backed or sponsored insurance for employers, landlords and others who provide jobs, apartments or other valuable statuses to offenders should be considered.* The availability of this kind of insurance might well promote reentry and reduce the risks that employers and landlords currently bear.

The information environment has changed. Social and legal trends suggest that, before long, all criminal history record information will be publicly available. Not only is that information likely to be available but it is likely that criminal history records will soon be just a mouse click away. The challenge will be to capture the benefits that flow from immediate, reliable and convenient access to criminal history record information while, at the same time, protecting offenders’ privacy and their ability to successfully reenter society.

Bob Belair, a founding partner of Oldaker, Biden & Belair, LLP, helped establish the Center for Privacy Research and Strategy, a privacy consulting firm.

This paper was commissioned by the National Center for Victims of Crime to inform the discussion of the Panel on Technology as a Community Engagement Tool for Crime Prevention. The commissioned papers provide detailed analyses of issues related to information privacy, the handling of criminal history record information, the impact of technology on police–community relations, and e-Government. For more information, visit www.ncvc.org/ict.