

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.